ÜBER

EINE KLASSE UNTERGRUPPEN EINER ABEL'SCHEN G_{nm}.

INAUGURAL-DISSERTATION

VON

JOSEF ANDERSSON

UPPSALA 1913
ALMQVIST & WIKSELLS BOKTRYCKERI-A.-B.

ÜBER EINE KLASSE UNTERGRUPPEN EINER ABEL'SCHEN G_{nm}.

INAUGURAL-DISSERTATION

ZUR

ERLANGUNG DER DOKTORWÜRDE

MIT GENEHMIGUNG

DER MATHEMATISCH-NATURWISSENSCHAFTLICHEN SEKTION
DER WEITBERÜHMTEN PHILOSOPHISCHEN FAKULTÄT
ZU UPPSALA

ZUR ÖFFENTLICHEN BEURTEILUNG VORGELEGT

ACAD.
LUGD.BAT.
BIBL.

VON

JOSEF ANDERSSON
LIC. PHIL., G—H.

DIE VERTEIDIGUNG WIRD AM 5. APRIL 1913
UM 10 UHR VORMITTAGS
IM HÖRSAL Nr. I STATTFINDEN

UPPSALA 1913
ALMQVIST & WIKSELLS BOKTRYCKERI-A.-B.

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41523710_0030

Für stetes Interesse während meiner Studien und manchen guten Rat bin ich meinen geehrten Lehrern, den Herren Professoren A. Wiman und E. Holmgren, zu aufrichtigem Danke verpflichtet. Es ist mir eine Freude, dies hier aussprechen zu dürfen.

Betreffs der Litteratur verweise ich auf imprimitive Gruppen in der Encyklopädie. Spezielle H-Gruppen treten in solchen als »heads» auf. Insbesondere sind zu nennen Aufsätze von Miller und Kuhn in Amer. J. of Math. 21, 26.

ARKIV FÖR MATEMATIK, ASTRONOMI OCH FYSIK.
BAND 8. N:o 37.

Über eine Klasse Untergruppen einer Abel'schen G_{n^m}.

Von

J. ANDERSSON.

Mitgeteilt am 22. Januar 1913 durch A. WIMAN und I. BENDIXSON.

Es seien $\Sigma_0 = (1^{(0)}\, 2^{(0)} \ldots n^{(0)})$,

$\Sigma_1 = (1^{(1)}\, 2^{(1)} \ldots n^{(1)})$,

$\Sigma_{m-1} = (1^{(m-1)}\, 2^{(m-1)} \ldots n^{(m-1)})$

m Operationen der Ordnung n, die eine ABEL'sche $G_{n^m} = [\Sigma_0, \Sigma_1, \ldots, \Sigma^{m-1}]$ erzeugen. Die folgende Untersuchung bezieht sich auf diejenigen Untergruppen von G_{n^m}, welche *bei zyklischer Vertauschung der Σ-Indices invariant sind. Ich nenne eine solche Gruppe eine H-Gruppe.* Diese H-Gruppen sind, besonders in den Fällen, wo m eine Primzahl oder das Produkt zweier Primzahlen ist, von Bedeutung für die Konstruktion der auflösbaren Permutationsgruppen in $m \,.\, n$ Elementen.

Die zyklische Vertauschung der Σ-Indices wird auch durch Transformation mit $C = (1^{(0)}\, 1^{(1)} \ldots 1^{(m-1)})\,(2^{(0)}\, 2^{(1)} \ldots 2^{(m-1)}) \ldots (n^{(0)}\, n^{(1)} \ldots n^{(m-1)})$ bewirkt, und diese Auffassung der Vertauschung ist aus mehreren Gründen zweckmässig.

Kommt die Operation O in einer H-Gruppe vor, so müssen $C^{-1}OC$, $C^{-2}OC^2, \ldots, C^{-(m-1)}OC^{m-1}$ und überhaupt jede $O^{a_0}C^{-1}O^{a_1}C \ldots C^{-(m-1)}O^{a_{m-1}}C^{m-1}$ oder $\prod_i C^{-i}O^{a_i}C^i$ in der

Gruppe enthalten sein. Ich bezeichne mit $\Phi(\alpha_i, O)$ oder $\Phi(O)$ die Operation $\prod_i C^{-i} O^{\alpha_i} C^i$. *Andererseits ist* $[O, C^{-1}OC, \ldots, C^{-(m-1)}OC^{m-1}]$ *offenbar eine H-Gruppe, die ich kürzer mit* $[\Phi(O)]$ *bezeichne.*

Man kann Φ, von der besonderen Wahl der Operation O unabhängig, als Symbol der kombinierten Transformationen und Zusammensetzungen auffassen, durch welche O in $\Phi(O)$ übergeht. In diesem Sinne spreche ich im Folgenden von »Anwendung des Symbols Φ» und verstehe also darunter die Herleitung von $\Phi(O)$ aus O. Es gibt n^m verschiedene Φ. Für gewisse O sind auch die $\Phi(O)$ alle verschieden, im allgemeinen aber werden mehrere $\Phi(O)$ gleich ausfallen. Die Ordnung der Gruppe $[\Phi(O)]$ ist dann $< n^m$.

Es seien $\Phi_1(\alpha_i)$ und $\Phi_2(\beta_i)$ zwei Symbole. Die nach einander folgenden Anwendungen von Φ_1 und Φ_2 liefern eine Operation, die ich mit $\Phi_2(\Phi_1(O))$ bezeichne. Da $\Phi_2(\Phi_1(O))$ in $[\Phi(O)]$ enthalten ist, muss

$\Phi_2(\Phi_1(O)) = \Phi_3(O)$, wo Φ_3 ein Symbol derselben Art ist. Für die Rechnung mit den Φ gelten folgende Regeln, die sich aus der Vertauschbarkeit der Σ_i ergeben:

(1) $$\text{I.} \quad \Phi(O_1 \,.\, O_2) = \Phi(O_1) \,.\, \Phi(O_2)$$

(2) $$\text{II.} \quad \Phi(\alpha_i, O) \,.\, \Phi(\beta_i, O) = \Phi(\alpha_i + \beta_i, O).$$

Es ist

$$\Phi_2(\Phi_1(O)) = \prod_j C^{-j} [\prod_i C^{-i} O^{\alpha_i} C^i]^{\beta_j} C^j$$

Nach (1) ist aber

$$\prod_j C^{-j} [\prod_i C^{-i} O^{\alpha_i} C^i]^{\beta_j} C^j = \prod_i \prod_j C^{-j} (C^{-i} O^{\alpha_i} C^i)^{\beta_j} C^j$$

$$= \prod_i \prod_j C^{-(i+j)} O^{\alpha_i \beta_j} C^{i+j} = \prod_i \prod_j C^{-i} (C^{-j} O^{\beta_j} C^i)^{\alpha_i} C^i$$

$$= \text{(nochmals nach (1))} \prod_i C^{-i} [\prod_j C^{-j} O^{\beta_j} C^j]^{\alpha_i} C^i = \Phi_1(\Phi_2(O)).$$

Als dritte Regel haben wir also

(3) $$\text{III.} \quad \Phi_1(\Phi_2(O)) = \Phi_2(\Phi_1(O)).$$

Aus (1) folgt $\Phi(\alpha_i, O^r) = [\Phi(\alpha_i, O)]^r$ und aus (2) $[\Phi(\alpha_i, O)]^r = \Phi(r\alpha_i, O)$. Folglich ist

$$\Phi(\alpha_i, O^r) = \Phi(r\alpha_i, O) = [\Phi(\alpha_i, O)]^r. \tag{4}$$

Ist nun die Ordnung von $[\Phi(O)] < n^m$, so können die $\Phi(O)$ nicht alle verschieden sein. Ist aber $\Phi(\alpha_i, O) = \Phi(\beta_i, O)$, so folgt nach (4) und (1)

$$\Phi(\alpha_i, O) \,.\, [\Phi(\beta_i, O)]^{-1} = \Phi(\alpha_i - \beta_i, O) = 1.$$

Die Φ für welche $\Phi(O) = 1$, bezeichne ich mit $\bar{\Phi}$ und nenne sie *»zur Gruppe $[\Phi(O)]$ gehörig»*. Diese Eigenschaft ist von O unabhängig, denn nach (3) ist $\bar{\Phi}(\Phi(O)) = \Phi(\bar{\Phi}(O)) = \Phi(1) = 1$. Es sei N die Anzahl der $\bar{\Phi}$. Dann sind von den übrigen $\Phi(O)$ je N gleich und zwar ist $\Phi(\alpha_i, O) = \bar{\Phi}(\alpha_i, O) \,.\, \Phi(\alpha_i, O) = \Phi(\alpha_i + \bar{\alpha}_i, O)$ für alle $\bar{\Phi}$. Die $\bar{\Phi}$ stehen in unmittelbarer Beziehung zu den Gruppencharakteren von $[\Phi(O)]$, wie sich später ergeben wird.

Nach diesem Bemerkungen gehen wir nun zur Untersuchung der in G_{n^m} enthaltenen H-Gruppen über.

Ich lasse die Operation

$$O = \Sigma_0^{\alpha_0} \Sigma_1^{\alpha_1} \cdots \Sigma_{m-1}^{\alpha_{m-1}} = \prod_i \Sigma_i^{\alpha_i}$$

dem Polynome

$$O(X) = \alpha_0 + \alpha_1 \,.\, X + \cdots + \alpha_{m-1} \,.\, X^{m-1}$$

entsprechen.

Die n^m Operationen O und die n^m modulis n, $X^m - 1$ verschiedenen Polynome sind dadurch ein-eindeutig auf einander bezogen. Diese Beziehung wird mit $O \sim O(X)$ bezeichnet.

Die Zusammensetzung der O entspricht der Addition modulo n der $O(X)$.

Wenn $O \sim O(X)$, so ist $C^{-1} O C \sim X \,.\, O(X)$ und allgemein $\Phi(\alpha_i, O) \sim (\alpha_0 + \cdots \alpha_{m-1} X^{m-1}) \,.\, O(X)$, wo das Polynom modulis n, $X^m - 1$ genommen wird.

Ich lasse nun auch das Symbol Φ dem Polynome $\Phi_x = \alpha_0 + \alpha_1 X + \cdots \alpha_{m-1} \,.\, X^{m-1}$ entsprechen. Auch die Φ_x hat man modulis n, $X^m - 1$ zu nehmen.

Wenn $\Phi' \sim \Phi'_x$, $\Phi'' \sim \Phi'''_x$, so ist $\Phi''' = \Phi'(\Phi'') = \Phi''(\Phi') \sim \Phi'_x . \Phi''_x$ modulis $n, X^m - 1$, wobei die Operation O, auf welche es nicht ankommt, weggelassen ist.

Wie das Operieren mit den O der Addition der $O(X)$ entspricht, so entspricht das Operieren mit den Φ der Multiplikation der Φ_x. Die oben gefundene Regel III, (3), folgt dann sofort. Die den Φ entsprechenden Φ_x besitzen Gruppeneigenschaft bei Addition, denn

$$\Phi(\alpha_i, O) . \Phi(\beta_i, O) = \Phi(\alpha_i + \beta_i, O) = 1.$$

Dies wird auch durch die später zu erörternde Beziehung zu den Gruppencharakteren nahegelegt.

I. Die Ordnung n der Σ_i eine Primzahl.

Es sei H eine beliebige H-Gruppe, O_1 eine darin vorkommende Operation und $O_1(X)$ das entsprechende Polynom. H enthält dann die Gruppe $[\Phi(O_1)]$. $[\Phi(O_1)] \sim (\alpha_0 + \alpha_1 X + \cdots \alpha_{m-1} X^{m-1}) O(X)$ (modulis $n, X^m - 1$) für $\alpha_0, \alpha_1, \ldots, \alpha_{m-1} = 0, 1, \ldots, n-1$. Hat nun $O(X)$ keinen Faktor modulo n mit $X^m - 1$ gemein, so können die α_i derart bestimmt werden, dass $(\alpha_0 + \cdots \alpha_{m-1} X^{m-1}) O(X) \equiv 1$ (modulis n, $X^m - 1$) wird. Es gibt ja zwei Polynome $G_1(X)$ und $G_2(X)$, für welche $1 \equiv G_1(X) . O(X) + G_2(X)(X^m - 1)$ (mod. n) identisch befriedigt ist. Dabei braucht man $G_1(X)$ nur modulo $X^m - 1$ zu nehmen. In diesem Falle enthält also H die Operation Σ_0 und $H = [\Phi(\Sigma_0)] = [\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}]$. Wir haben daher als erstes Resultat: *Ist die Ordnung einer H-Gruppe $< n^m$, muss jedes $O(X)$ einen Faktor modulo n von $X^m - 1$ enthalten.* Den in $O_1(X)$ aufgehenden Faktor setze ich nun $= \frac{X^m - 1}{F_1}$, wo F_1 vom Grade $\varkappa_1$ ist und $F_1 . \frac{X^m - 1}{F_1} \equiv X^m - 1$ (mod. n).

Ist H mit $[\Phi(O_1)]$ nicht erschöpft, nehme man eine zweite in $[\Phi(O_1)]$ nicht vorkommende Operation O_2. Der in O_2 aufgehende Faktor modulo n von $X^m - 1$ sei $\frac{X^m - 1}{F_2}$, wo F_2 vom Grade $\varkappa_2$ ist. So fährt man fort, bis H erschöpft ist. Es seien

$$\frac{X^m-1}{F_1}, \frac{X^m-1}{F_2}, \ldots, \frac{X^m-1}{F_r}$$

die gefundenen Faktoren modulo n von X^m-1. F_i vom Grade $\varkappa_i$.

$$[\Phi(O_i)] \sim (\alpha_0 + \cdots \alpha_{m-1} X^{m-1}) \cdot \frac{X^m-1}{F_i}$$

hat die Ordnung $n^{\varkappa_i}$. Denn

$$(\alpha_0 + \cdots \alpha_{m-1} X^{m-1}) \frac{X^m-1}{F_i} = (\alpha_0 + \cdots \alpha_{m-1} X^{m-1}) \frac{X^m-1}{F_i} +$$

$$+ G \cdot (X^m-1) \equiv (\alpha_0 + \cdots \alpha_{m-1} X^{m-1} + G \cdot F_i) \frac{X^m-1}{F_i}$$

$$(\text{modulis } n, X^m-1),$$

und nach zweckmässiger Wahl von G werden $\alpha_{\varkappa_i}, \alpha_{\varkappa_{i+1}}, \ldots, \alpha_{m-1} \equiv 0 \pmod{n}$. Nun ergibt sich der Satz:

Es ist immer möglich eine Operation O in H so auszuwählen, dass $[\Phi(O)] = H$ wird. Eine solche Operation ist

$$\bar{O} \sim \frac{X^m-1}{\bar{F}}, \text{ wo } \frac{X^m-1}{\bar{F}} \tag{5}$$

vom Grade $m-n$ der *grösste gemeinschaftliche Teiler modulo* n von

$$\frac{X^m-1}{F_1}, \frac{X^m-1}{F_2}, \ldots, \frac{X^m-1}{F_r}$$

ist. *Ich nenne den Faktor F zur Gruppe H gehörig.* $[\Phi(\bar{O})]$ ist mit H identisch, wenn a) H in $[\Phi(O)]$ enthalten ist und auch b) $[\Phi(\bar{O})]$ in H.

a). Ist ohne weiteres klar, da jedes $(\alpha_0 + \cdots \alpha_{\varkappa_i-1} X^{\varkappa_i-1}) \frac{X^m-1}{F_i}$ auch von der Form $(\alpha_0 + \cdots \alpha_{\bar{\varkappa}-1} \cdot X^{\bar{\varkappa}-1}) \frac{X^m-1}{\bar{F}}$ ist.

b). H enthält alle O, welche

$$(\alpha_0^{(1)} + \cdots \alpha_{m-1}^{(1)} X^{m-1}) \frac{X^m-1}{F_1} + \cdots + (\alpha_0^{(r)} + \cdots \alpha_{m-1}^{(r)} X^{(m-1)}) \frac{X^m-1}{F_r}$$

entsprechen. Hierin können aber die $a^{(1)}, a^{(2)}, \ldots, a^{(r)}$ so gewählt werden, dass die Summe den Wert $\frac{X^m-1}{F}$ modulo n erhält, und damit ist auch die zweite Behauptung erwiesen.

Man kann offenbar $O(X)$ durch irgend ein $O'(X) = G(X)O(X)$ ersetzen, wo $G(X)$ modulo n zu X^m-1 teilerfremd ist, ohne dass die Gleichung $H = [\Phi(O')]$ zu gelten aufhört, aber unter diesen $O'(X)$ ist $O(X)$ als vom möglichst kleinen Grade bevorzugt. Die einzigen $O(X)$ vom Grade $m-z$ sind die $k \,.\, O(X)$, $k = 1, 2, \ldots, n-1$. Die entsprechenden O sind: $\bar{O}, \bar{O}^2, \ldots, \bar{O}^{n-1}$. Das zuletzt Bewiesene kann man auch so ausdrücken: *In jeder H_{n^z}-Gruppe gibt es eine Basis $\bar{O}, C^{-1}\bar{O}C, \ldots, C^{-(z-1)}\bar{O}C^{z-1}$, wo in $\bar{O}$ $\Sigma_{m-z+1}, \Sigma_{m-z+2}, \ldots \Sigma_{m-1}$ fehlen;* durch diese Basis ist die H_{n^z} eindeutig bestimmt und vice versa. Zusammenfassend können wir sagen: *Die Bestimmung der in $[\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}]$ enthaltenen H-Gruppen ist ein mit der Zerlegung von X^m-1 in modulo n irreduzible Faktoren äquivalentes Problem.*

Die zu einer H-Gruppe gehörigen Φ können wir jetzt bestimmen. Ist F der zu H gehörige Faktor vom Grade z, d. h.

$$H_{n^z} \sim (\alpha_0 + \cdots + \alpha_{z-1} X^{z-1}) \frac{X^m-1}{F},$$

so entsprechen die Φ den Polynomen $\Phi_x = (\alpha_0 + \alpha_1 X + \cdots + \alpha_{m-z-1} X^{m-z-1}) F$. Denn es ist $\Phi(O) \sim \bar{\Phi}_x \,.\, O(X) \equiv 0$ (modulis n, X^m-1) für alle O in H_{n^z}. Die Anzahl der Φ ist n^{m-z}. Aus den für alle O in H_{n^z} identisch erfüllten $\Phi(O) = 1$ berechnet man dann *die zur Gruppe H gehörigen Charaktere.*[1] Ein Charakter $\varepsilon_0^{\beta_0} \varepsilon_1^{\beta_1} \ldots \varepsilon_{m-1}^{\beta_{m-1}}$, wo die ε n^{te} Einheitswurzeln sind, gehört zur Gruppe H_{n^z}, wenn für jede $O = \Pi \Sigma_i^{\alpha_i}$ in H_{n^z}

$$\varepsilon_0^{\alpha_0 \cdot \beta_0} \cdot \varepsilon_1^{\alpha_1 \cdot \beta_1} \ldots \varepsilon_{m-1}^{\alpha_{m-1} \cdot \beta_{m-1}} = 1 \text{ oder}$$

(6)

$$\alpha_0 \beta_0 + \alpha_1 \beta_1 + \cdots \alpha_{m-1} \beta_{m-1} \equiv 0 \pmod{n}.$$

Wir haben nun $\Phi(\beta_i, O) = \Phi(\beta_i, \Pi_i \Sigma_i^{\alpha_i}) = 1$ für alle O. Daraus

[1] Siehe WEBER, Algebra II, §§ 13, 14.

$$\begin{aligned}
&\alpha_0\beta_0 + \alpha_{m-1}\cdot\beta_1 + \cdots + \alpha_1\cdot\beta_{m-1} \equiv 0 \pmod{n}\\
&\alpha_1\beta_0 + \alpha_0\cdot\beta_1 + \cdots + \alpha_2\cdot\beta_{m-1} \equiv 0 \pmod{n} \qquad (7)\\
&\qquad\qquad\cdots\cdots\cdots\cdots\cdots\cdots\\
&\alpha_{m-1}\cdot\beta_0 + \alpha_{m-2}\beta_1 + \cdots + \alpha_0\beta_{m-1} \equiv 0 \pmod{n}
\end{aligned}$$

Diese Kongruenzen besagen aber nach (6), dass $\varepsilon_0^{\beta_0}\varepsilon_1^{\beta-1}\ldots\varepsilon_i^{\beta-i}\ldots\varepsilon_{m-1}^{\beta_1}$ und die daraus durch zyklische Verschiebung der ε-Indices hervorgehenden Charaktere zur Gruppe H_{n^x} gehörig sind. Man erhält sie alle, wenn man dem Polynom $\Phi_x = \Sigma\beta_i X$ den Charakter $\Pi\varepsilon_i^{\beta-i}$ entsprechen lässt. Diese $\Pi\varepsilon_i^{\beta-i}$ bilden bei der Komposition durch Multiplikation eine Gruppe der Ordnung n^{m-x}, »die reziproke zu H_{n^x}», *die auch bei zyklischer Vertauschung der ε-Indices invariant ist.* Die Kongruenzen (7) müssen gültig bleiben auch nach Ersatz von α_{-i} durch α_{-i-1}, weil auch $\Phi(C^{-1}OC) = 1$. Dieselbe Veränderung bewirkt aber der Ersatz von β_{-i} durch β_{-i-1} oder von ε_{i+1} durch ε_i in $\Pi\varepsilon_i^{\beta-i}$. Es sind also $\Pi\varepsilon_i^{\gamma i}$ und $\Pi\varepsilon_{i+1}^{\gamma i}$ gleichzeitig zur Gruppe H_{n^x} gehörige Charaktere.

Das könnte man auch folgern aus *dem Verhalten der H-Gruppen bei den relativ zyklischen Vertauschungen der Σ-Indices.* Wie C bei Transformation die Substitution $i' \equiv i+1 \pmod{m}$ der Σ-Indices bewirkt, entsprechen die auf analoge Weise gebildeten $c_1, c_2, \ldots$ den Substitutionen

$$i' \equiv g_1 i \pmod{m},\ i' \equiv g_2 i \pmod{m}, \ldots, \text{ wo } g_1, g_2, \ldots$$

eine Basis der Gruppe der zu m relativ primen Zahlklassen[1] ist. $[C_1 c_1, c_2, \ldots]$ ist dann mit der relativ zyklischen Gruppe in m Elementen einstufig isomorph. Es ist nun von vornherein klar, dass $c^{-1}Hc$ *auch eine H-Gruppe ist* für jede Operation c in $[C_1 c_1, c_0, \ldots]$. Denn aus

$$C^{-1}HC = H$$

folgt

$$c^{-1}C^{-1}c\,.\,c^{-1}Hc\,.\,c^{-1}Cc = c^{-1}Hc.$$

[1] Siehe Weber, Algebra II, § 18.

Da aber $c^{-1} C c = C^g$, wo g zu m relativ prim ist, folgt $C^{-g} c^{-1} H c\, C^g = c^{-1} H c$, d. h. $c^{-1} H c$ ist eine H-gruppe. Lässt man

$$\Phi_x = (\alpha_0 + \cdots \alpha_{m-\varkappa-1} X^{m-\varkappa-1}) F = \sum_{i=0}^{i=m-1} \beta_i X^i \text{ (modulis } n, X^m - 1)$$

dem Charakter $\Pi \varepsilon_i^{\beta_i}$ entsprechen, so bilden diese $\Pi \varepsilon_i^{\beta_i}$ eine bei zyklischer Vertauschung der ε-Indices invariante Gruppe. Dasselbe muss dann für $\Pi \varepsilon_i^{\beta_{-i}}$ gelten, welche die zu H reziproke Gruppe bilden, und durch die relativ zyklische Vertauschung $i' \equiv -i \pmod m$ aus $\Pi \varepsilon_i^{\beta_i}$ hervorgehen.

Ist n nicht in m als Faktor enthalten, gilt allgemein:

Jede H-Gruppe ist bei der Vertauschung $i' \equiv ni \pmod m$ der Σ-Indices invariant.

Wenn

$$O = \Pi \Sigma_i^{a_i} \sim \alpha_0 + \alpha_1 X + \cdots \alpha_{m-1} X^{m-1} = O(X),$$

so ist

$$O' = \Pi \Sigma_{ni}^{a_i} \sim \alpha_0 + \alpha_1 X^n + \cdots \alpha_{m-1} X^{n(m-1)} = O(X^n).$$

Aber

$$O(X^n) \equiv [O(X)]^n \equiv [O(X)]^{n-1} . O(X) \pmod n,$$

d. h. O' ist in $[\Phi(O)]$ enthalten.

$X^m - 1$ ist das Produkt der Polynome $X_{\varphi(m_1)} = X^{\varphi(m_1)} + \alpha_1 X^{\varphi(m_1)-1} + \cdots \alpha_{\varphi(m_1)}$, wo m_1 alle Teiler von m durchläuft und $X_{\varphi(m_1)} = 0$ von den $\varphi(m_1)$ primitiven Einheitswurzeln befriedigt ist.[1] *Wenn nun n in m nicht aufgeht*, gibt es eine kleinste Zahl $\varkappa_{m_1}$, für welche

$$n^{\varkappa_{m_1}} \equiv 1 \pmod{m_1} \text{ ist.}$$

$X_{\varphi(m_1)}$ zerfällt dann bekanntlich modulo n in $\frac{\varphi(m_1)}{\varkappa_{m_1}}$ verschiedene, irreduzible Faktoren $F_1, F_2, \ldots$ vom Grade $\varkappa_{m_1}$, und zwar kann man

$$F_i \equiv (X - \varepsilon^i)(X - \varepsilon^{in}) \ldots (X - \varepsilon^{in^{\varkappa_{m_1}-1}}) \pmod n$$

[1] Siehe WEBER, Algebra I, § 141.

setzen, wenn ε eine primitive m_1^{te} Einheitswurzel ist.[1] Das gilt nun für jeden Teiler m_1 von m, und die so erhaltenen modulo n irreduziblen Faktoren von $X^m - 1$ sind alle verschieden. Es sei $X^m - 1 \equiv F_1 . F_2 \ldots F_s$ (modulo n). F_i hat den Grad z_i; es ist $n^{z_i} \equiv 1$ (mod. m_1), wenn F_i in $X_{\varphi(m_1)}$ aufgeht.

Besonders einfacher Art müssen nun die H-Gruppen sein, zu welchen die irreduziblen Polynome F_i gehören. Zuerst bemerken wir, dass *alle H-Gruppen als Produkt solcher Gruppen darstellbar sind.* Denn ist

$$H \sim (\alpha_0 + \cdots \alpha_{z-1} X^{z-1}) \frac{X^m - 1}{F_1 . F_2 \ldots F_r},$$

(vgl. (5))

$$\overset{(i)}{H}_{n^{z_i}} \sim (\alpha_0 + \cdots \alpha_{z_i - 1} X^{z_i - 1}) \frac{X^m - 1}{F_i},$$

so ist

$$H = \overset{(1)}{H} . \overset{(2)}{H} \ldots \overset{(r)}{H}.$$

Das folgt wie oben (5), da $\dfrac{X^m - 1}{F_1 \ldots F_r}$ der grösste gemeinschaftliche Teiler von $\dfrac{X^m - 1}{F_1}, \dfrac{X^m - 1}{F_2}, \ldots, \dfrac{X^m - 1}{F_r}$ ist. *Insbesondere ist* $[\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}] = \overset{(1)}{H} . \overset{(2)}{H} \ldots \overset{(s)}{H}$, *woraus die Unmöglichkeit von* $1 = O_1 . O_2 \ldots O_s$ *für von* 1 *verschiedene* O_i (O_i in $\overset{(i)}{H}$) *folgt.* Die Ordnung der rechtstehenden Gruppe muss ja den höchsten Wert $n^{z_1 + z_2 + \cdots z_s} = n^m$ wirklich erreichen. Aus der Verschiedenheit der F_i folgt ferner: *Es gibt* Φ, *die zu allen* $\overset{(i)}{H}$ *mit Ausnahme einer einzigen gehören.* $\Phi \sim \dfrac{X^m - 1}{F_i}$ z. B. gehört zu allen ausser $\overset{(i)}{H}$.

Die Φ_x verteilen sich modulo F_i auf n^{z_i} Restklassen. Die Φ_x der Klasse 0 entsprechen den Φ. Für Φ_x aus derselben Restklasse sind die $\Phi(O)$ gleich. Solche Φ werden nicht als verschieden betrachtet. Die so bestimmten Φ entsprechen den modulis n, F_i verschiedenen Polynomen Φ_x, die jetzt auch als Galois'sche Imaginären aufgefasst werden können.

[1] Vgl. WEBER, Algebra II, S. 744.

Aus der Existenz von Primitivzahlen folgt dann: *Man kann immer ein Φ so auswählen, dass die Operationen von $H_{n^{\varkappa_i}}$ alle in der Reihe* $1, \Phi(O), \Phi^2(O), \ldots, \Phi^{n^{\varkappa_i-2}}(O)$ *enthalten sind.*

Wir zeigen ferner, dass *jede* $\overset{(i)}{H}_{n^{\varkappa_i}}$

(8) $$n-1 \text{ Operationen } O^*, O^{*2}, \ldots, O^{*n-1}$$

enthält, die bei der Vertauschung $i' \equiv ni \pmod m$ *der Σ-Indices invariant sind.* Es sei $c^{-1}\Sigma_i c = \Sigma_{ni}$. Dann wird

$$c^{-1}\Phi(O)c = c^{-1}(\prod_i C^{-i}O^{a_i}C^i)\,c = \prod_i C^{-ni}(c^{-1}Oc)^{a_i}C^{ni}.$$

Φ_x geht also in $\Phi_{x^n} = (\Phi_x)^n \pmod n$ über. Ist nun $c^{-1}Oc = \Phi^a(O)$, folgt

$$c^{-1}\Phi(O)c = \Phi^n(\Phi^a(O)) = \Phi^{n+a}(O) \text{ und allgemein}$$

$$c^{-1}\Phi^x(O)c = \Phi^{nx+a}(O). \text{ Man kan nun } x$$

so wählen, dass $c^{-1}\Phi^x(O)c = \Phi^x(O)$ wird. Dazu ist erforderlich:

(9) $$nx + a \equiv x \pmod{n^{\varkappa_i} - 1}.$$

a ist aber durch $n-1$ teilbar. Nach $\varkappa_i$-maliger Wiederholung ergibt sich ja

$$c^{-\varkappa_i}\Phi^x(O)c^{\varkappa_i} = \Phi^{n^{\varkappa_i}\cdot x + a\cdot\frac{n^{\varkappa_i-1}}{n-1}}(O).$$

Da $c^{\varkappa_i} = 1$, muss also $a\cdot\dfrac{n^{\varkappa_i}-1}{\varkappa-1} \equiv 0 \pmod{n^{\varkappa_i}-1}$ sein. Dann hat aber (9) wie behauptet $n-1$ Lösungen. Ebenso folgert man, *dass die Anzahl der mit* $c^\delta : i' \equiv n^\delta i$ *(mod. m) vertauschbaren Operationen in* $\overset{(i)}{H}_{n^{\varkappa_i}}$ $n^\delta - 1$ *ist* (δ ein Faktor von $\varkappa_i$).

Ist F_i ein Faktor von $X_{\varphi(m_1)}$, $m_1 < m$, und

$$\overset{(i)}{H}_{n^{\varkappa_i}} \sim (\alpha_0 + \cdots + \alpha_{\varkappa_i-1}X^{\varkappa_i-1})\frac{X^m-1}{F_i},$$

sind alle Operationen in $H_{n^{\varkappa_i}}$ *von der Form*

$$(10)\qquad \left(\Sigma_0\Sigma_{m_1}\Sigma_{2m_1}\dots\Sigma_{\left(\frac{m}{m_1}-1\right)m_1}\right)^{\beta_0}\left(\Sigma_1\Sigma_{1+m_1}\dots\Sigma_{1+\left(\frac{m}{m_1}-1\right)m_1}\right)^{\beta_1}\dots$$
$$(\Sigma_{m_1-1}\Sigma_{2m_1-1}\dots\Sigma_{m-1})^{\beta_{m_1-1}}.$$

Man hat in der Tat für jede O

$$C^{-m_1}OC^{m_1}O^{-1}\sim(X^{m_1}-1)O(X)\equiv 0 \text{ (modulis } n, X^m-1), \text{ d. h.}$$

O ist mit C^{m_1} vertauschbar. Die $\overset{(i)}{H}_{n^{\varkappa_i}}$, für welche F_i in $X^{m_1}-1$ aufgeht, können also sofort hingeschrieben werden, wenn in $[\Sigma_0, \Sigma_1, \dots, \Sigma_{m_1-1}]$ die H-Gruppen, bestimmt sind.

Wir haben oben (8) gezeigt, dass jede H-Gruppe bei der Vetauschung $i' \equiv ni \pmod m$ der Σ-Indices invariant ist. Nun suchen wir alle Vertauschungen $i' \equiv gi \pmod m$,[1] welche eine unsrer $\overset{(i)}{H}_{n^{\varkappa_i}}$ ungeändert lassen. Zu dem Zwecke bemerken wir zuerst, dass *eine* $\overset{(i)}{H}$, *für welche* F_i *in* $X_{\varphi(m_1)}$ *aufgeht, in jede* $\overset{(i)}{H}$, *welche einem der übrigen Faktoren* $F_{i'}$ *von* $X_{\varphi(m_1)}$ *entspricht, durch Vertauschungen der* Σ*-Indices von der Form* $i' \equiv \gamma i$ *(mod. m) überführbar ist.* Sind nämlich

$$F_i = \left(X-\varepsilon^{\frac{m}{m_1}}\right)\left(X-\varepsilon^{\frac{m}{m_1}\cdot n}\right)\dots\left(X-\varepsilon^{\frac{m}{m_1}\cdot n^{\varkappa_i-1}}\right) \pmod n$$

$$F_{i'} = \left(X-\varepsilon^{\frac{m}{m_1}\cdot\gamma}\right)\left(X-\varepsilon^{\frac{m}{m_1}\cdot\gamma\cdot n}\right)\dots\left(X-\varepsilon^{\frac{m}{m_1}\cdot\gamma\cdot n^{\varkappa_i-1}}\right) \pmod n$$

und $\gamma\gamma' \equiv 1 \pmod{m_1}$, so geht F_i, wenn man X durch $X^{\gamma'}$ ersetzt, in

$$F_{i''} = \left(X^{\gamma'}-\varepsilon^{\frac{m}{m_1}\cdot\gamma\cdot\gamma'}\right)\dots \pmod n \text{ über.}$$

$F_{i''}$ hat aber den Faktor $F_{i'}$ und mithin geht $\overset{(i)}{H}$ in $\overset{(i')}{H}$ durch die Vertauschung $i' \equiv \gamma' i \pmod m$ der Σ-Indices über.[2] Die Anzahl der in $X^{m_1}-1$ aufgehenden F_i ist $\frac{\varphi(m_1)}{\varkappa_i}$. Nun bleibt nach (10) $\overset{(i)}{H}_{n^{\varkappa_i}}$ ungeändert bei allen $i' \equiv gi \pmod m$, für welche $g \equiv 1 \pmod{m_1}$. Die Zahl dieser Substitutionen ist,

[1] g muss natürlich zu m relativ prim sein.

[2] Es lässt sich sogar jede Operation $(\not\equiv 1)$ in etwa $\overset{(i)}{H}$ in eine andere $\overset{(i')}{H}$ überführen, welche in einer beliebigen $\overset{(i')}{H}$ enhalten ist.

wie man leicht findet, $\frac{\varphi(m)}{\varphi(m_1)}$.[1] $n^{\varkappa_1}$ ist die erste Potenz von n, welche $\equiv 1 \pmod{m}$. *Die Substitutionen* $i' \equiv gi \pmod{m_1}$ *mit* $g \equiv 1 \pmod{m_1}$ *und* $i' \equiv ni \pmod{m}$ *erzeugen also eine Gruppe der Ordnung* $\varkappa_i \cdot \frac{\varphi(m)}{\varphi(m_1)}$, *welche die gesuchte ist.* Sie hat ja als Untergruppe von $G_{q(m)}$, welche alle $i' \equiv gi \pmod{m}$ enthält, den Index $\frac{\varphi(m_1)}{\varkappa_i}$, wie es nach dem oben Bewiesenen sein muss.

Wir wollen nun die H-Gruppen etwas genauer untersuchen, deren zugehöriger Faktor F eines der modulo n irreduziblen Polynome ist, in welche $X_{q(m)}$ zerfällt. Es sei $m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_r^{a_r}$ und $n^{\varkappa_1} \equiv 1 \pmod{p_1^{a_1}}$, $n^{\varkappa_2} \equiv 1 \pmod{p_2^{a_2}} \cdots$. Die F sind dann vom Grade $\varkappa$, wo $\varkappa$ die kleinste Zahl ist, in welcher $\varkappa_1, \varkappa_2, \varkappa_3 \ldots$ aufgehen. Die Exponenten α_i der in

$$H_{n^\varkappa} \sim (\beta_0 + \beta_1 X + \cdots \beta_{\varkappa-1} X^{\varkappa-1}) \cdot \frac{X^m - 1}{F}$$

enthaltenen Operationen $O = \Pi \Sigma_i^{\alpha_i}$ müssen gewisse Bedingungen erfüllen. Setzt man in $O(X)$ $X^{m_1} = 1$, $X^{m_1+k} = X^k$, so wird $O(X) \equiv 0$ (modulis n, $X^m - 1$) für alle m_1. Dies besagt aber, dass

$$\begin{aligned}
&\alpha_0 + \alpha_{m_1} + \alpha_{2m_1} + \cdots \equiv 0 \pmod{n} \\
&\alpha_1 + \alpha_{1+m_1} + \alpha_{1+2m_1} + \cdots \equiv 0 \pmod{n} \\
&\quad \cdots \cdots \cdots \cdots \cdots \\
&\alpha_{m_1-1} + \alpha_{2m_1-1} + \alpha_{3m_1-1} + \cdots \equiv 0 \pmod{n}.
\end{aligned}$$

Insbesondere gelten diese Kongruenzen für $m_1 = \frac{m}{p_1}, \frac{m}{p_2}, \ldots$. Sie sind nicht alle von einander unabhängig. Die Anzahl der unabhängigen Bedingungen muss $m - \varphi(m)$ sein. Wenn $\alpha_i + \alpha_{i+\frac{m}{p_1}} + \cdots \equiv \alpha_i + \alpha_{i+\frac{m}{p_2}} + \cdots \equiv \cdots \equiv 0 \pmod{n}$, so gehört also $\Pi \Sigma_i^{\alpha_i}$ gewiss zu einer der H, deren F in $X_{\varphi(m)}$ aufgeht.

Es sei $H_{n^{\varkappa_i}}$ eine der in $\left[\Sigma_0, \Sigma_1, \ldots, \Sigma_{p^{a_i-1}}\right]$ enthaltenen

[1] Siehe WEBER, Algebra II, § 18.

H-Gruppen, für welche der Faktor F vom Grade $\varkappa_i$ in $X_{\varphi(p_1^{a_1})}$ aufgeht, und $O^{(i)} = \Sigma_0^{a_0^{(i)}} \Sigma_1^{a_1^{(i)}} \cdots \Sigma_{p_i^{a_{i-1}}}^{p_i^{a_i^{(i)}}}$ eine Operation dieser Gruppe. Die Operationen in unserer $H_{n^\varkappa}$ können nun aus solchen $O^{(i)}$ zusammengeflochten werden in folgender Weise: Ich setze

$$[O^{(1)}, O^{(2)}, \ldots, O^{(r)}] = \prod_{i_1} \prod_{i_2} \ldots \prod_{i_r} \Sigma_{i_1, i_2, \ldots i_r}^{a_{i_1}^{(1)} \cdot a_{i_2}^{(2)} \cdot a_{i_r}^{(r)}};$$

i_1 geht von 0 bis $p_1^{a_1} - 1$ u. s. w. Unter $\Sigma_{i_1, i_2, \ldots, i_r}$ verstehe ich Σ_i für

$$i \equiv i_1 \cdot \frac{m}{p_1^{a_1}} + i_2 \cdot \frac{m}{p_2^{a_2}} + \cdots i_r \cdot \frac{m}{p_r^{a_r}} \pmod{m}.$$

Sämtliche i sind in dieser Form enthalten für $i_1 = 0, 1, \ldots$ $p_1^{a_1} - 1$ u. s. w. Die durch Kombination aller $O^{(1)}$, $O^{(2)}$, .., entstehenden $[O^{(1)}, O^{(2)}, \ldots, O^{(r)}]$ erzeugen eine Gruppe

$$H_{n^{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r}} = [(O^{(1)}, O^{(2)}, \ldots, O^{(r)})],$$

von welcher wir nachweisen wollen:

1. *$H_{n^{\varkappa_1 \ldots \varkappa_r}}$ ist eine in*

$$H_{n^{\varphi(m)}} \sim (\alpha_0 + \cdots \alpha_{\varphi(m)-1} X^{\varphi(m)-1}) \frac{X^m - 1}{X_{\varphi(m)}}$$

enthaltene H-Gruppe von der Ordnung $n^{\varkappa_1 \cdots \varkappa_r}$.

2. *$H_{n^{\varphi(m)}}$ ist das Produkt aller $\frac{\varphi(p_1^{a_1})}{\varkappa_1} \cdot \frac{\varphi(p_2^{a_2})}{\varkappa_2} \cdots \frac{\varphi(p_r^{a_r})}{\varkappa_r}$ $H_{n^{\varkappa_1 \ldots \varkappa_r}}$ und jede $H_{n^{\varkappa_1 \ldots \varkappa_r}}$ enthält somit $\frac{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r}{\varkappa}$ verschiedene $H_{n^\varkappa}$.*

1 Um zu zeigen, dass für eine der erzeugenden Operationen

$$[O^{(1)}, O^{(2)}, \ldots, O^{(r)}] = \Pi \Sigma_i^{a_i} = \prod_{i_1} \prod_{i_2} \ldots \prod_{i} \Sigma_{i_1 \ldots i}^{a_{i_1}^{(1)} \cdot a_{i_2}^{(2)} \ldots a_{i_7}^{(r)}}$$

$$\alpha_i + \alpha_{i+\frac{m}{p_1}} + \cdots \alpha_{i+(p_1-1)\frac{m}{p_1}} \equiv 0 \pmod{n} \text{ ist,}$$

genügt es $i_2, i_3, \ldots i_r$ bei der Summation festzuhalten. Die Behauptung folgt dann aus der entsprechenden Eigenschaft der $O^{(1)}$. Dasselbe gilt für $\frac{m}{p_2}, \frac{m}{p_3}, \ldots,$ und $H_{n^{\varkappa_1}\ldots\varkappa_r}$ gehört somit zu $H_{n^{\varphi(m)}}$. Dass sie eine H-Gruppe ist, folgt daraus, dass die erzeugenden Operationen nur unter sich vertauscht werden bei Transformation mit $C^{\frac{m}{p_1^{a_1}}}, C^{\frac{m}{p_2^{a_2}}}, \ldots,$ wie leicht aus $i \equiv i_1 \cdot \frac{m}{p_1^{a_1}} + i_2 \cdot \frac{m}{p_2^{a_2}} + \cdots \pmod{m}$ zu schliessen ist. Wenn ferner $O_1^{(i)}, O_2^{(i)}, O_{j_i}^{(i)}, \ldots, O_{\varkappa_i}^{(i)}$ eine Basis der Gruppe $H_{n^{\varkappa_i}}$ ist, so lassen sich die erzeugenden $[O^{(1)}, O^{(2)}, \ldots, O^{(r)}]$ alle durch $[O_{j_1}^{(1)}, O_{j_2}^{(2)}, \ldots, O_{j_r}^{(r)}]$ $(j_1 = 1, 2, \ldots, \varkappa_1,$ u. s. w.) ausdrücken. Dies folgt durch Wiederholung aus $[O^{(1)}, O^{(2)}, \ldots, O_1^{(i)}, \ldots, O^{(r)}]$ $[\ldots, O_2^{(i)}, \ldots] = [\ldots, O_1^{(i)} \cdot O_2^{(i)}, \ldots]$, eine Gleichheit, welche sofort aus der Produktform von $[O^{(1)}, O^{(2)}, \ldots, O^{(r)}]$ resultiert. Die $\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r$ $[O_{j_1}^{(1)}, O_{j_2}^{(2)}, \ldots, O_{j_r}^{(r)}]$ bilden übrigens eine Basis der Gruppe $H_{n^{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r}}$, welche also die Ordnung $n^{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r}$ hat. Diese Behauptung beweisen wir durch Induktion. Wir nehmen als richtig an, dass die $\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_{r-1}$ $[O_{j_1}^{(1)}, O_{j_2}^{(2)}, \ldots, O_{j_{r-1}}^{(r-1)}]$ $(j_i = 1, 2, \ldots \varkappa_i)$ eine Basis von $H_{n^{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_{r-1}}}$ sind. Wäre nun unsere Behauptung falsch, müsste eine Gleichheit

$$1 = \Pi [O_{j_1}^{(1)}, O_{j_2}^{(2)}, \ldots, O_{j_r}^{(r)}]^{\lambda_{j_1, j_2, \ldots, j_r}} \text{ gelten.}$$

$O_1^{(r)}$ möge in k verschiedenen $[O_{j_1}^{(1)}, \ldots, O_1^{(r)}]$ mit den Exponenten $\lambda_1, \lambda_2 \ldots, \lambda_k$ vorkommen. Ich bezeichne diese Operationen mit $[O]^{\lambda_1}, [O]^{\lambda_2}, \ldots [O]^{\lambda_k}$. Sammeln wir nun die Exponenten von $\Sigma_{i_1, i_2, \ldots, 0}$, $\Sigma_{i_1, i_2, \ldots, 1}$, $\ldots$ bei festgehaltenen $i_1, i_2, \ldots i_{r-1}$, so sind diese, wenn

$$O_j^{(r)} = \prod_{i=0}^{p_r^{a_r}-1} \Sigma_i^{\nu_i(j)}$$

ist, von der Gestalt $(A_1\lambda_1 + A_2\lambda_2 + \cdots A_k\lambda_k)\alpha_0^{(1)} + \cdots$,

$$(A_1\lambda_1 + A_2\lambda_2 + \cdots A_k\lambda_k)\alpha_1^{(1)} + \cdots,$$

$$\cdots\cdots\cdots\cdots,$$

wo die fehlenden Glieder in entsprechender Weise von $[O_{j_1}^{(1)}, O_{j_2}^{(2)}, \ldots, O_{\cdot}^{(r)}] \ldots$ herrühren. Wegen der Basiseigenschaft von $O_1^{(r)}, O_2^{(r)}, \ldots$ muss nun $A_1\lambda_1 + A_2\lambda_2 + \cdots A_k\lambda_k \equiv 0 \pmod{n}$ sein d. h. schon $[O]^{\lambda_1}.[O]^{\lambda_2} \ldots [O]^{\lambda_k} = 1$. Um so mehr ist diejenige Operation mit der Einheit identisch, die aus allen in $[O]^{\lambda_1} \ldots [O]^{\lambda_k}$ vorkommenden $\Sigma_{i_1, i_2, \ldots i_{r-1}, 0}$ besteht. Setzen wir ferner voraus, dass $\alpha_0^{(1)}$ in $O_1^{(r)} = \delta \neq 0$, was wir nötigen Falls durch eine Transformation mit $C^{k \cdot \frac{m}{p_r^{a_r}}}$ bewirken können, so wird die fragliche Operation $\prod_{i=1}^{k} \left[O_{j_1}^{(1)}, O_{j_2}^{(2)}, \ldots, O_{j_{r-1}}^{r-1}\right]^{\lambda_i \delta} = 1$. Dies ist aber mit unserer Voraussetzung in Widerspruch.

2. Aus Operationen in den $\frac{\varphi(p_i^{a_i})}{\varkappa_i} H_{n^{\varkappa_i}}$ lässt sich eine bei allen Vertauschungen $i' \equiv g_i i \pmod{p_i^{a_i}}$ invariante Operation O_i zusammensetzen. In dem Produkte der $\frac{\varphi(p_1^{a_1}) \cdot \varphi(p_2^{a_2}) \ldots \varphi(p_r^{a_r})}{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r}$ verschiedenen $H_{n^{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r}}$ kommt nun auch $[O_1, O_2, \ldots, O_r]$ vor. Diese Operation ist bei allen relativ zyklischen Vertauschungen der Σ-Indices invariant. Somit[1] enthält das Produkt aller $H_{n^{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r}}$ die Gruppe $H_{n^{\varphi(m)}}$ und ist, da die Ordnungen übereinstimmen, mit dieser Gruppe identisch. Wir schliessen ferner, dass jede $H_{n^{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r}}$ das Produkt von $\frac{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r}{\varkappa}$ verschiedenen $H_{n^\varkappa}$ ist. *Sind* $\varkappa_1, \varkappa, \ldots \varkappa_r$ *teilerfremd, ist* $\varkappa = \varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r$ *und* $H_{n^{\varkappa_1 \cdot \varkappa_2 \ldots \varkappa_r}} = H_{n^\varkappa}$ d. h. die Bestimmung der $H_{n^\varkappa}$ für ein beliebiges m ist auf die Bestimmung der $H_{n^\varkappa}$ für $m = p^a$ zurückgeführt.

Setzt man andererseits die $H_{n^\varkappa}$ *oder die Zerlegung von* $X_{\varphi(m)}$ *modulo n als bekannt voraus, so können daraus die entsprechenden* $H_{n^{\varkappa'}}$ *für jeden Teiler* m' *von* m *abgeleitet werden,*

[1] Die fragliche $\overline{O}$ ist in der Form $O_1 \cdot O_2 \ldots O_{\varphi(m)}^{\varkappa}$ darstellbar, wo alle $H_{n^\varkappa}$ vertreten sind (vgl. S. 11, Fussnote 2). Dann sind alle $H_{n^\varkappa}$ in $[\Phi(O)]$ enthalten (S. 9).

wie wir jetzt nachweisen wollen. Wir beschränken uns auf den Fall $m' = \frac{m}{p_1}$, weil dann die Wiederholung desselben Verfahrens zu einem beliebigen Teiler m' führt. *Es sei zuerst* $a_1 > 1$ *d. h.* m' *durch* p_1 *teilbar.* $n^\varkappa \equiv 1 \pmod{m}$, $n^{\varkappa'} \equiv 1 \pmod{m'}$. Denken wir uns nun in allen Operationen einer $H_{n^\varkappa}$ die Σ, deren Index nicht durch p_1 teilbar ist, weggewischt, so bilden die in dieser Weise geänderten Operationen eine mit $H_{n^\varkappa}$ isomorphe Gruppe H. H bleibt ferner invariant bei Transformation mit C^{p_1} und ist also, *wenn* Σ_i *statt* Σ_{ip_1} *geschrieben wird,* eine in $[\Sigma_0, \Sigma_1, \ldots, \Sigma_{m'-1}]$ enthaltene H-Gruppe. Der zugehörige Faktor geht in $X_{\varphi(m')}$ auf, weil die Exponenten α_{ip_1} die Bedingungen

$$\begin{aligned}
&\alpha_{ip_1} + \alpha_{i.p_1+\frac{m}{p_1}} + \cdots \quad \alpha_{ip_1+(p-1)\cdot\frac{m}{p_1}} \equiv 0 \pmod{n},\\
&\alpha_{ip_1} + \alpha_{ip_1+\frac{m}{p_2}} + \cdots \qquad\qquad \equiv 0 \pmod{n},\\
&\qquad\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&\alpha_{ip_1} + \alpha_{ip_1+\frac{m}{p_r}} + \cdots \qquad\qquad \equiv 0 \pmod{n},
\end{aligned}$$

erfüllen. Zwei Möglichkeiten sind nun zu unterscheiden:

1. $\varkappa' = \varkappa$.
2. $\varkappa' < \varkappa$.

1. H ist notwendig mit einer, der in $[\Sigma_0, \Sigma_1, \ldots, \Sigma_{m'-1}]$ enthaltenen $H_{n^{\varkappa'}}$ identisch, wenn Σ_i statt Σ_{ip_1} geschrieben wird, da die Ordnung dem Isomorphismus mit $H_{n^\varkappa}$ zufolge $< n^\varkappa$ ist.

2. Da m' durch p_1 teilbar ist, folgert man leicht, dass $\varkappa = p.\varkappa'$. Ist nun O' eine Operation in $H_{n^{\varkappa'}}$, und wird jedes Σ_i durch Σ_{ip} ersetzt, so ist, wenn O die so erhaltene Operation bezeichnet,

$$\begin{aligned}
&[\overline{O},\ C^{-p}\,\overline{O}\,C^{p},\ C^{-2p}\,\overline{O}\,C^{2p}, \ldots\ C^{-(\varkappa'-1)p}\,\overline{O}\,C^{(\varkappa'-1)p},\\
&C^{-1}OC,\ C^{-(p+1)}OC^{p+1},\ C^{-(2p+1)}OC^{2p+1}, \ldots\ C^{-[(\varkappa'-1)p+1]}\overline{O}\,C^{(\varkappa'-1)p+1},\\
&\qquad\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&C^{-(p-1)}OC^{p-1},\ C^{-(2p-1)}\,\overline{O}\,C^{2p-1}, \ldots\ C^{-(\varkappa' p-1)}\,\overline{O}\,C^{\varkappa' p-1}]
\end{aligned}$$

offenbar eine in $[\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}]$ enthaltene H-Gruppe, deren zugehöriger Faktor ausserdem in $X_{\varphi(m)}$ aufgeht. Da die Ord-

nung $n^{p\cdot x'} = n^x$ ist, muss also die fragliche Gruppe mit einer der H_{n^x} zusammenfallen. Daraus folgt dann umgekehrt, *dass*, genau wie im Falle 1, *eine* H_{n^x}, *resultiert, falls alle* Σ_{ip} *durch* Σ_i *ersetzt werden und alle übrigen* Σ *in den Operationen der* H_{n^x} *fortgelassen werden.* Die obige Darstellung der H_{n^x} hängt damit zusammen, dass $X_{\varphi(p.m')}$ aus $X_{\varphi(m')}$ hervorgeht, wenn X^p statt X geschrieben wird.[1] *Jetzt nehmen wir* $a_1 = 1$, *d. h. m und m' teilerfremd an.* Die m Operationen Σ können folgendermassen geordnet werden:

$$\Sigma_{0,0}\ \Sigma_{1,0}\ \ldots\ \Sigma_{m'-1,0},$$

$$\Sigma_{0,1}\ \Sigma_{1,1}\ \ldots\ \Sigma_{m'-1,1},$$

$$\ldots\ldots\ldots$$

$$\Sigma_{0,p-1}\ \Sigma_{1,p-1}\ \ldots\ \Sigma_{m'-1,p-1},$$

wo Σ_{i_1,i_2} für $\Sigma_{i_1.p+i_2.m'}$ steht. Die Operationen $[O^{(1)}, O^{(2)}, \ldots, O^{(r)}]$ bezeichne ich kürzer mit $[O^{(1)}, O^{(m')}]$, wo $O^{(m')}$ eine beliebige Operation in $H_{n^{x_2.x_3\ldots x_r}}$ bedeutet. $H_{n^{x_2.x_3\ldots x_r}} = H^{(1)}_{n^{x'}}.H^{(2)}_{n^{x'}}\ldots H^{(x_2\ldots x_r)}_{n^{x'}}$ und demgemäss ist $O^{(m')} = \bar{O}_1.\bar{O}_2\ldots$, *wo* $\bar{O}_i$ *zu* $H^{(i)}_{n^{x'}}$ *gehört.* Wenn endlich $O_i^{(0)}, O_i^{(1)}, O_i^{(2)}, \ldots$ diejenige Operation bezeichnet, welche aus O_i entsteht, wenn $\Sigma_{ip}, \Sigma_{m'+ip}, \Sigma_{2m'+ip}\ldots$ bzw. statt Σ_i geschrieben wird, so ist die allgemeine Form einer Operation in $H_{n^{x_1.x_2\ldots x_r}}$:

$$O = \Pi O_i^{(0)}.\Pi P_i^{(1)}\ldots.$$

Ist nun O in einer H_{n^x} enthalten, so beweisen wir, dass $\Pi\bar{O}_i$, $\Pi P_i, \ldots$ in einer $H_{n^{x'}}$ enthalten sind. Dies besagt aber, dass wir auch in diesem Falle ganz auf dieselbe Weise wie oben von m zu $m' = \frac{m}{p}$ herabsteigen können. Die Anwendung des Symbols $\prod_{i=1}^{i=m'} C^{-pi}[\ ]^{a_i} C^{pi}$ auf O ist offenbar mit der Anwendung von $\prod_{i=1}^{i=m'} C^{-i}[\ ]^{a_i} C^{i}$ auf $O^{(m')}$ in $O = [O_1^{(1)},$

[1] m' *muss* dabei durch p teilbar sein.

$O_1^{(m')}][O_2^{(1)}, O_2^{(m')}]\ldots$ gleichwertig. Nun gibt es immer ein Symbol Φ, für welches $\Phi(\bar{O}_1) = 1$, $\Phi(\bar{O}_2) = \Phi(O_3) = \cdots = 1$. Enthält nun in $O = \Pi O_i^{(0)} \cdot \Pi P_i^{(1)} \ldots$ etwa $\Pi \bar{O}_i^{(0)}$ mehrere $\bar{O}_i^{(0)} : \bar{O}_1^{(0)}, \bar{O}_2^{(0)}, \ldots$, so folgt durch Anwendung dieses Φ, dass H_{n^x} eine Operation O' enthält, in welcher die den $\Pi \bar{O}_i^{(0)}$, $\Pi \bar{P}_i^{(1)} \ldots$ entsprechenden $O^{(m')}$ alle zu $H_{n^{x'}}^{(1)}$ gehören. Dann ist aber $[O', C^{-1} O' C, C^{-2} O' C^2, \ldots]$ eine in H_{n^x} enthaltene H-Gruppe, deren Ordnung nicht n^x erreichen kann, was unmöglich ist. Es ist ja immer $\Pi C^{-i} O'^{a_i} C^i$ von der Form:

$$\bar{O}_1^{(0)} \cdot \bar{P}_1^{(1)} \cdot \bar{Q}_1^{(2)} \ldots,$$

wo $\bar{O}_1, \bar{P}_1, \bar{Q}_1 \ldots$ Operationen in $H_{n^{x'}}^{(1)}$ sind; die Operation $O = O_1^{(0)} O_2^{(0)} \ldots$ kann also nicht auftreten, und die Ordnung muss $< n^x$ sein.

Ist $m = n^r \cdot m_1$ d. h. m und n nicht relativ prim, so ist $X^m - 1 \equiv (X^{m_1} - 1)^{n^r} \pmod{n}$, und es genügt die Zerlegung von $X^{m_1} - 1$ modulo n auszuführen. Wir nehmen nun m und n teilerfremd an und wollen die Zerlegung von $X^m - 1$ modulo n etwas genauer untersuchen.

m eine Primzahl p.

Es sei $n^x \equiv 1 \pmod{p}$. Dann zerfällt $X^p - 1$ in $(X-1) F_0 \cdot F_1 \ldots F_{\frac{p-1}{x}-1}$, wo F_i modulo n irreduzible Polynome, alle vom Grade x sind. Die entsprechenden Gruppen sind: $[\Sigma_0 \Sigma_1 \ldots \Sigma_{p-1}]$, $H_{n^x}^{(0)}, H_{n^x}^{(1)}, \ldots, H_{n^x}^{\left(\frac{p-1}{x}-1\right)}$. Es genügt eine einzige Operation in einer dieser $H_{n^x i}^{(i)}$ zu kennen, denn daraus können durch Vertauschungen der Form $i' \equiv \gamma i \pmod{p}$ Operationen in den übrigen H_{n^x} hergeleitet werden. Am einfachsten gelingt wohl die Bestimmung einer der Operationen O^*, die bei der Vertauschung $i' \equiv n i \pmod{p}$ der Σ-Indices invariant sind. Wir gehen von dem Ansatze:

$$O^* = (\Sigma_0 \Sigma_n \Sigma_{n^2} \dots \Sigma_{n^{\varkappa-1}})^{\alpha_0} (\Sigma_\gamma \Sigma_{\gamma \cdot n} \dots \Sigma_{\gamma \cdot n^{\varkappa-1}})^{\alpha_1} \dots$$

(11)

$$\cdot \left(\Sigma_{\gamma^{\frac{p-1}{\varkappa}-1}} \Sigma_{\gamma^{\frac{p-1}{\varkappa}-1} \cdot n} \dots \Sigma_{\gamma^{\frac{p-1}{\varkappa}-1} \cdot n^{\varkappa-1}} \right)^{\alpha_{\frac{p-1}{\varkappa}-1}} \cdot \Sigma_0^{-\varkappa\left(\alpha_0+\alpha_1 \dots +\alpha_{\frac{p-1}{\varkappa}-1}\right)}$$

aus.[1] Es muss die Exponentensumme $\equiv 0$ modulo n sein. Es muss ferner

$$\Phi_0(O^*) = \prod_{i=0}^{i=\varkappa-1} C^{-n^i} O^* C^{n^i} = O^{*\varrho}, \tag{12}$$

weil $\Phi_0(O^*)$ in $H_{n^\varkappa}$ enthalten ist und bei der Vertauschung $i' \equiv n\,i \pmod{p}$ ungeändert bleibt. Durch Vergleichung der Exponenten in $\Phi_0(O^*)$ und $O^{*\varrho}$ entstehen die linearen Kongruenzen:

$$\begin{aligned}
&A_{00}\alpha_0 + A_{10}\alpha_1 + \cdots A_{N0}\alpha_N \equiv \varrho \cdot \alpha_0 \pmod{n},\\
&A_{01}\alpha_0 + A_{11}\alpha_1 + \cdots A_{N1}\alpha_N \equiv \varrho \cdot \alpha_1 \pmod{n},\\
&\qquad\qquad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \qquad (13)\\
&A_{0N}\alpha_0 + A_{1N}\alpha_1 + \cdots A_{NN}\alpha_N \equiv \varrho \cdot \alpha_N \pmod{n},\\
&\varkappa \cdot \alpha_i \equiv -\varrho \cdot \varkappa \cdot (\alpha_0 + \alpha_1 \cdots + \alpha_N) \pmod{n},
\end{aligned}$$

wo N statt $\frac{p-1}{\varkappa} - 1$ geschrieben ist. α_i in der letzten Kongruenz ist dadurch bestimmt, dass die Reihe $-1, -n, -n^2, \dots, -n^{\varkappa-1}$ mit $\gamma^i, \gamma^i n, \dots, \gamma^i \cdot n^{\varkappa-1}$ identisch sein muss, oder, was dasselbe besagt, es ist $i \equiv \frac{p-1}{2} \left(\text{mod. } \frac{p-1}{\varkappa}\right)$. Zuerst muss nun eine der Kongruenzen (13) eine Folge der übrigen sein. Multipliziert man in den N ersten beiderseits mit $\varkappa$ und addiert, so folgt $0 \equiv 0$, da auf der linken Seite die Exponentensumme von $\Pi\, C^{-n^i} O^* C^{n^i}$ nur in anderer Verteilung steht. Damit die N ersten Kongruenzen (13) ein gemeinschaftliches Lösungssystem besitzen, muss ϱ die Bedingung

[1] γ eine primitive Wurzel von p.

$$(14) \qquad \begin{vmatrix} A_{00}-\varrho & A_{10} & \dots & A_{N0} \\ A_{01} & A_{11}-\varrho & & A_{N1} \\ \dots & \dots & \dots & \dots \\ N_{NN} & & & N_{NN}-\varrho \end{vmatrix} \equiv 0 \pmod{n}$$

erfüllen. Aus (13) erhält man dann die Verhältnisse $\alpha_0 : \alpha_1 : \dots : \alpha_N$. (11) wird von allen $O_0^*, O_1^*, \dots O_N^*, O_i^*$ in $H_{n^\varkappa}^{(i)}$, befriedigt. Die entsprechenden Lösungen sind $\alpha_0 : \alpha_1 : \dots : \alpha_N \equiv \alpha_0 : \alpha_1 : \dots : \alpha_N$, $\alpha_N : \alpha_0 : \dots : \alpha_{N-1}, \dots, \alpha_1 : \alpha_2 : \dots : \alpha_0$. Hat das System (13) nur $\frac{p-1}{\varkappa}$ Lösungen, so sind diese notwendig die gesuchten. Unter Umständen ist aber die Zahl der Lösungen grösser und zwar hat (14) dann mehrfache Wurzeln. Die Bedeutung der Wurzeln $\varrho_0, \varrho_1, \dots, \varrho_N$ von (14) ist die folgende: Es muss, wie aus der Theorie der GALOIS'schen Imaginären bekannt ist, das zu Φ_0 gehörige $\Phi_{0X} = X + X^n + \cdots X^{n^{\varkappa-1}}$ mit einer Zahl ϱ_i modulis n, F_i kongruent sein. Diese Zahlen ϱ_i sind die Wurzeln von (14). Ist nun ϱ_i eine einfache Wurzel von (14), so hat (13) für $\varrho = \varrho_i$ eine bestimmte Lösung $\alpha_0 : \alpha_1 : \dots : \alpha_N$, welche O_i^* entspricht. Denn die allgemeinste Lösung von (13): $\prod_{i=0}^{i=N} (\Sigma_{\gamma^i} \Sigma_{\gamma^{i+n}} \dots \Sigma_{\gamma^{i+n^{\varkappa-1}}})^{a_i} \cdot \Sigma^{-\frac{p-1}{\varkappa}(a_0+a_1\dots+a_N)}$ ist auch in der Form $\Pi O_i^{*\beta_i}$ darstellbar. Es ist aber $\Phi_0 (\Pi_i O_i^{*\beta_i}) = \Pi_i \Phi_0 (O_i^{*\beta_i}) = \Pi_i O_i^{*\varrho_i \cdot \beta_i}$, und daraus folgt, dass $\beta_0 = \beta_1 = \dots = \beta_{i-1} = \beta_{i+1} = \dots = \beta_N = 0$ für $\varrho = \varrho_i$ in (13), wenn ϱ_i einfache Wurzel von (14) ist. Ist aber $\varrho_a = \varrho_b = \cdots \varrho_g$, so sind alle $O_a^{*\beta_0} O_b^{*\beta_1} \dots O_g^{*\beta_g}$ für $\beta_a, \beta_b, \dots, \beta_g = 0, 1, \dots, n-1$ Lösungen von (13). Unter den Lösungen des Systems (13) für $\varrho = \varrho_a$ *muss es also g verschiedene* $\alpha_0 : \alpha_1 : \dots : \alpha_N$ *geben, welche durch zyklische Verschiebungen in einander übergehen.* Aber noch mehr. Ist $\varkappa$ nicht durch n teilbar und setzt man $\alpha_i \equiv \varrho_a$, so folgt leicht $\alpha_{i+1} \equiv \varrho_{a+1}$, $\alpha_{a+2} \equiv \varrho_{a+2}$ u. s. w. Es ist also für eine Lösung, welche einer O^* entspricht,

$$(15) \qquad \alpha_0 : \alpha_1 : \dots : \alpha_N \equiv \varrho_{a-i} : \varrho_{a-i+1} : \dots : \varrho_a : \varrho_{a+1} : \varrho_{a-i-1},$$

wo die i modulo $\frac{p-1}{\varkappa}$ zu nehmen sind. i in α_i ist durch

$i \equiv \frac{p-1}{2} \left(\text{mod. } \frac{p-1}{\varkappa}\right)$ bestimmt, und zwar ist $i = 0$ oder $\frac{p-1}{2\varkappa}$, je nachdem $\varkappa$ gerade oder ungerade ist. Für mässig grosse n ist es gewöhnlich leicht mit Hilfe dieser Kriterien die Lösungen, welche O^* entsprechen, herauszufinden. Um die Richtigkeit von (15) einzusehen genügen folgende Bemerkungen:

1. Ist $\Phi_0 X \equiv \varrho_i$ (modulis n, F_i), so muss

$$\Phi_i X \equiv \varrho_i \text{ (modulis } n, F_0). \tag{16}$$

Aus $\Phi_0 X \equiv X + X^n + \cdots + X^{n^{\varkappa-1}} = \varrho_i + G_1 . F_i + n . G_2$ folgt, wenn man X^{γ^i} an Stelle von X schreibt

$$\Phi_i X = \varrho_i + G'_1 . F_0 + n . G'_2.$$

Es ist ja $F_i \equiv (X - \varepsilon^{\gamma^i})(X - \varepsilon^{\gamma^i . n}) \ldots (X - \varepsilon^{\gamma^i . n^{\varkappa-1}})$ (mod. n), und $(X^{\gamma^i} - \varepsilon^{\gamma^i})(X^{\gamma^i} - \varepsilon^{\gamma^i . n}) \ldots$ hat den Faktor

$$F_0 \equiv (X - \varepsilon)(X - \varepsilon^n) \ldots$$

2. Wie in (12) wird $\Phi_i(O^*) = O^{*\varrho_i}$, wenn $\Phi_0(O^*) = O^{*\varrho_0}$, und

$$\varkappa . \alpha_j \equiv -\varrho_i \varkappa (\alpha_0 + \alpha_1 + \cdots + \alpha_N), \tag{13'}$$

wo j aus

$$j \equiv i + \frac{p-1}{2} \left(\text{mod. } \frac{p-1}{\varkappa}\right)$$

bestimmt ist. Diese Art des Schliessens versagt, wenn $\varkappa$ durch n teilbar ist.[1] (15) gilt aber auch in diesem Falle. Wir werden später sehen, dass es auch, wenn die Ordnung der Σ eine Primzahlpotenz ist, analoge H-Gruppen mit Operationen $O^*, O^{*2}, \ldots$ gibt. Ist $\varkappa$ durch n^r teilbar, so nimmt man die Ordnung der $\Sigma = n^{r+1}$ und erhält für die Bestimmung der O^* ein System derselben Art wie (13). In der letzten Kongruenz kann beiderseits der Faktor n^r entfernt werden,

[1] $\alpha_0 + \alpha_1 + \cdots + \alpha_N$ ist immer $\not\equiv 0$ (mod. n).

und dann gilt die Kongruenz modulo n. Die so gefundenen α_i sind aber mit den α_i in (13) identisch, da jede O^* von der n^{ten} Ordnung die $n^{r\text{te}}$ Potenz einer O^* der $n^{r+1\text{ten}}$ Ordnung ist.

Aus (16) folgt, dass (14) modulo n mit der aus der Theorie der Gleichung $X^p - 1 = 0$ bekannten Periodengleichung der $\varkappa$-gliedrigen Perioden zusammenfällt. Dieser Umstand gestattet einige Schlüsse etwas allgemeinerer Natur in den Fällen $\varkappa = \frac{p-1}{2}, \frac{p-1}{3}, \frac{p-1}{4}$.

$\varkappa = \frac{p-1}{2}$. Es seien $O_1 = \Sigma_1 \Sigma_n \dots \Sigma_{n^{\frac{p-1}{2}-1}}$,

$$O_2 = \Sigma_\gamma \cdot \Sigma_{\gamma n} \dots \Sigma_{\gamma \cdot n^{\frac{p-1}{2}-1}},$$

$$O^* = O_1^{\alpha} O_2^{\beta} \Sigma_0^{-\frac{p-1}{2}(\alpha+\beta)},$$

$$(17) \quad \Phi_0(O^*) = \Pi C^{-n^i} O_1^{\alpha} O_2^{\beta} \Sigma_0^{-\frac{p-1}{2}(\alpha+\beta)} C^{n^i} =$$

$$= O_1^{\varrho_0 \alpha} O_2^{\varrho_0 \beta} \Sigma_0^{-\frac{p-1}{2}\varrho_0(\alpha+\beta)},$$

$$(18) \quad \Phi_1(O^*) = \Pi C^{-\gamma \cdot n^i} O_1^{\alpha} O_2^{\beta} \Sigma_0^{-\frac{p-1}{2}(\alpha+\beta)} C^{\gamma \cdot n^i} =$$

$$= O_1^{\varrho_1 \alpha} O_2^{\varrho_1 \beta} \Sigma_0^{-\frac{p-1}{2}\varrho_1(\alpha+\beta)},$$

$$(19) \quad \Pi C^{-n^i} O_1^{\beta} O_2^{\alpha} \Sigma_0^{-\frac{p-1}{2}(\alpha+\beta)} C^{n^i} =$$

$$= O_1^{\varrho_1 \beta} O_2^{\varrho_1 \alpha} \Sigma_0^{-\frac{p-1}{2}\varrho_1(\alpha+\beta)},$$

wo (19) aus (18) durch die Vertauschung $i' = \gamma i \pmod{p}$ der Σ-Indices hervorgeht.

Aus (17) und (18)

$$O_1^{-\alpha} O_2^{-\beta} \Sigma_0^{\frac{p-1}{2}(\alpha+\beta)} \prod_{i=0}^{i=p-1} C^{-i} O^* C^i =$$

$$= O_1^{(\varrho_0+\varrho_1)\alpha} O_2^{(\varrho_0+\varrho_1)\beta} \Sigma_0^{-(\varrho_0+\varrho_1)\frac{p-1}{2}(\alpha+\beta)},$$

woraus, da $\Pi C^{-i} O^* C^i = 1$,

(20) $$\varrho_0 + \varrho_1 \equiv -1 \pmod{n},$$

was auch aus der Periodengleichung folgt.

Aus (17) und (19)

$$H C^{-n^i} (\Sigma_0 \dots \Sigma_{p-1})^{\alpha+\beta} \Sigma_0^{-p(\alpha+\beta)} C^{n^i} = O_1^{\varrho_0\alpha+\varrho_1\beta} O_2^{\varrho_1\alpha+\varrho_0\beta} \Sigma_0^{\frac{p-1}{2}(\alpha+\beta)},$$

da $\varrho_0 + \varrho_1 \equiv -1 \pmod{n}$. Da ferner

$$H C^{-n^i} (\Sigma_0 \dots \Sigma_{p-1})^{\alpha+\beta} C^{n^i} = (O_1 O_2 \Sigma_0)^{\frac{p-1}{2}(\alpha+\beta)} \text{ und}$$

$$H C^{-n^i} \Sigma_0^{-p(\alpha+\beta)} C^{n^i} = O_1^{-p(\alpha+\beta)}, \text{ so folgen}$$

(21) $$\varrho_0\alpha + \varrho_1\beta \equiv \left(\frac{p-1}{2} - p\right)(\alpha+\beta) \pmod{n},$$

(22) $$\varrho_0\beta + \varrho_1\alpha \equiv \frac{p-1}{2}(\alpha+\beta) \pmod{n}.$$

Ist $p = 4h+1$, tritt Σ_{-1} in O_1 auf und $\alpha:\beta = \varrho_0:\varrho_1$, ist aber $p = 4h+3$, muss $\alpha:\beta = \varrho_1:\varrho_0$ sein. Im ersten Falle folgt aus (22) $\varrho_0\varrho_1 \equiv -\frac{p-1}{4}$, im zweiten aus (21) $\varrho_0\varrho_1 \equiv +\frac{p+1}{4}$. Die Periodengleichung modulo n wird also

$$\text{für } p = 4h+1 : \varrho^2 + \varrho + \frac{1-p}{4} \equiv 0 \pmod{n},$$

$$\text{für } p = 4h+3 : \varrho^2 + \varrho + \frac{1+p}{4} \equiv 0 \pmod{n}.$$

Diese Koeffizienten sind aber die tatsächlichen der Periodengleichung.[1] Man kann auch $\alpha:\beta = \left(\varrho + \frac{1-p}{2}\right) : \left(\varrho + \frac{1+p}{2}\right)$ setzen. Für $n=2$ muss $O^* = \Sigma_1 \Sigma_n \dots \Sigma_{n^{\frac{p-1}{2}}-1} \cdot \Sigma_0^{\frac{p-1}{2}}$ und $\Sigma_\gamma \Sigma_{\gamma \cdot n} \dots \Sigma_{\gamma \cdot n^{\frac{p-1}{2}}-1} \Sigma_0^{\frac{p-1}{2}}$.

$\varkappa = \frac{p-1}{3}$. Es ist $p = 6h+1$ und $\frac{p-1}{2} = 3h \equiv 0$

[1] Siehe WEBER, Algebra I, § 179.

$\left(\text{mod. } \frac{p-1}{\varkappa}\right)$. Σ_{-1} tritt also in $\Sigma_1 \Sigma_n \dots \Sigma_{n^{\frac{p-1}{3}}-1}$ auf. Genau wie oben $\left(\varkappa = \frac{p-1}{2}\right)$ folgen mit der Bezeichnung (11), (16),

$$\varrho_0 + \varrho_1 + \varrho_2 = -1, \tag{23}$$

$$\alpha_0 \varrho_0 + \alpha_1 \varrho_1 + \alpha_2 \varrho_2 \equiv (\alpha_0 + \alpha_1 + \alpha_2)\left[\frac{p-1}{3} - p\right] \text{ (mod. } n), \tag{24}$$

$$\alpha_0 \varrho_2 + \alpha_1 \varrho_0 + \alpha_2 \varrho_1 \equiv (\alpha_0 + \alpha_1 + \alpha_2)\ \frac{p-1}{3} \qquad \text{(mod. } n), \tag{25}$$

$$\alpha_0 \varrho_1 + \alpha_1 \varrho_2 + \alpha_2 \varrho_0 \equiv (\alpha_0 + \alpha_1 + \alpha_2)\ \frac{p-1}{3} \qquad \text{(mod. } n). \tag{26}$$

Setzen wir nun nach (15) $\alpha_0 : \alpha_1 : \alpha_2 = \varrho_0 : \varrho_1 : \varrho_2$, so ist aus (23), (25) ersichtlich, dass der Koeffizient von ϱ in der Periodengleichung mit $-\frac{p-1}{3}$ modulo n kongruent ist. Es ist freilich oft leicht, mit Benutzung gewisser zahlentheoretischer Eigenschaften der Koeffizienten[1] die Periodengleichung direkt aufzustellen, um aber unter den 6 möglichen Anordnungen $\varrho_0 : \varrho_1 : \varrho_2$ diejenigen drei herauszufinden, welche O^* entsprechen, ist eine besondere Nachprüfung erforderlich. Für $n = 2$ und 3 ist indessen die Kenntniss der Periodengleichung hinreichend. Nach (23) müssen die Wurzeln ϱ_0, ϱ_1, ϱ_2 für $n = 2$ mit den Zahlen 0, 0, 1 in irgend einer Reihenfolge übereinstimmen. Die Zahl der möglichen $\varrho_0 : \varrho_1 : \varrho_2$ sinkt auf 3 herab, und die O^* sind von der Form $\left(\Sigma_{\gamma^i} \Sigma_{\gamma^{i \cdot n}} \dots \Sigma_{\gamma^{i \cdot n^{\frac{p-1}{3}-1}}}\right) \Sigma_0^{-\frac{p-1}{3}}$. Für $n = 3$ können nach (23) die Wurzeln ϱ_0, ϱ_1, ϱ_2 nicht alle verschieden sein. Es muss also die Diskriminante der Periodengleichung durch 3 teilbar sein. Wir haben für die Wurzeln 3 Möglichkeiten:

1. $-1, -1, 1$; $\varrho_0 \varrho_1 + \varrho_1 \varrho_2 + \varrho_2 \varrho_0 \equiv -\frac{p-1}{3} \equiv -1 \text{ (mod. } 3)$,
2. $0, 1, 1$; » $\equiv$ » $\equiv 1$ (»),
3. $0, 0, -1$; » $\equiv$ » $\equiv 0$ (»).

[1] Siehe WEBER l. c. § 180.

Da $3^{\frac{p-1}{3}} \equiv 1 \pmod{p}$, ist $3^{\frac{p-1}{6}} \equiv -1 \pmod{p}$ und $3^{\frac{p-1}{3}+\frac{p-1}{6}} = 3^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. 3 ist also quadratischer Nichtrest von p.[1] Da ferner $p-1$ gerade und durch 3 teilbar ist, haben wir die 3 möglichen Formen für p:

1. $p = 36h + 31$; $-\frac{p-1}{3} \equiv -1 \pmod 3$; $O^* = O_0 O_1 O_2^{-1} . \Sigma_0^{-\frac{p-1}{3}}$.

2. $p = 36h + 7$; $-\frac{p-1}{3} \equiv 1 \pmod 3$; $O^* = O_0 O_1 . \Sigma_0^{\frac{p-1}{3}}$.

3. $p = 36h + 19$; $-\frac{p-1}{3} \equiv 0 \pmod 3$; $O^* = O_0$.

$O_i = \Sigma_{i^i} \Sigma_{i^i . n} \cdots \Sigma_{i^i . n^{\frac{p-1}{3}-1}}$. Die übrigen O^* durch zyklische Vertauschung der O_i. Die kleinsten p sind

1. $p = 67 = 36 + 31$; $4 . 67 = 5^2 + 243$,

2. $p = 151 = 36 . 4 + 7$; $4 . 151 = 19^2 + 243$,

3. $p = 1783 = 36 . 49 + 19$; $4 . 1783 = 83^2 + 243$.

Die Darstellbarkeit in der Form $A^2 + 243 . B^2$ von $4p$ ist eine notwendige Eigenschaft, die aus

$$3^{\frac{p-1}{3}} \equiv 1 \pmod{p} \text{ folgt.}^2$$

$\varkappa = \frac{p-1}{4}$. Es ist $p = 4h + 1$. $\frac{p-1}{2} = 2h \equiv 0, 2 \pmod 4$

je nachdem h gerade oder ungerade ist. Dem entsprechend kommt Σ_{-1} in O_0 oder O_2 vor.

Man hat wie für $\varkappa = \frac{p-1}{2}, \frac{p-1}{3}$,

$$\varrho_0 + \varrho_1 + \varrho_2 + \varrho_3 = -1, \tag{27}$$

[1] $\left(\frac{3}{p}\right) = -1$ für $p = 12h \pm 5$.

[2] Siehe WEBER, l. c. § 180. Die Diskriminante ist durch 3 teilbar.

$$(28)\quad \alpha_0\varrho_0+\alpha_1\varrho_1+\alpha_2\varrho_2+\alpha_3\varrho_3 = (\alpha_0+\alpha_1+\alpha_2+\alpha_3)\left(\frac{p-1}{4}-p\right) \pmod{n},$$

$$(29)\quad \alpha_0\varrho_{0+i}+\alpha_1\varrho_{1+i}+\alpha_2\varrho_{2+i}+\alpha_3\varrho_{3+i} \equiv (\alpha_0+\alpha_1+\alpha_2+\alpha_3)\frac{p-1}{4} \pmod{n},$$

für $i=1, 2, 3$. Für $p=8h+1$ ist nach (15) $\alpha_0:\alpha_1:\alpha_2:\alpha_3 = \varrho_0:\varrho_1:\varrho_2:\varrho_3$ und für $p=8h+5$ ist $\alpha_0:\alpha_1:\alpha_2:\alpha_3=\varrho_2:\varrho_3:\varrho_0:\varrho_1$.

Im ersten Falle folgt durch Addition der drei Kongruenzen (29) für $i=1, 2, 3$:

$$\varrho_0\varrho_1+\varrho_0\varrho_2+\varrho_0\varrho_3+\varrho_1\varrho_2+\varrho_1\varrho_3+\varrho_2\varrho_3 = \Sigma\varrho_i\varrho_j = -3\cdot\frac{p-1}{8} \pmod{n},$$

und im zweiten Falle ersetzt man (29) für $i=2$ durch (28) und erhält:

$$\varrho_0\varrho_1+\varrho_0\varrho_2+\cdots = \Sigma\varrho_i\varrho_j = -\frac{1}{2}\left[3\cdot\frac{p-1}{4}-p\right] = \frac{p+3}{8} \pmod{n}.$$

Der Koeffizient von ϱ^2 in der Periodengleichung ist also mit $-3\cdot\frac{p-1}{8}$ bzw. $\frac{p+3}{8}$ kongruent.[1] $n=2$. Die Wurzeln sind 0, 0, 0, 1 oder 0, 1, 1, 1. $\Sigma\varrho_i\varrho_j \equiv 0$ bzw. 1. Nun ist $2^{\frac{p-1}{4}} \equiv 1 \pmod{p}$ also $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ und $\left(\frac{2}{p}\right)=1$. Da $p-1$ durch 4 teilbar ist, muss folglich p von der Form $16h+1$ oder $16h+9$ sein. Der Koëffizient von ϱ^2 wird $-3\cdot 2h$ bzw. $-3\cdot(2h+1)$ d. h. $\equiv 0$ bzw. 1. *Für* $p=16h+1$ *ist also* O^* *vom Typus* $O_0\Sigma_0^{-\frac{p-1}{4}}$ und *für* $p=16h+9$ *vom Typus* $O_0O_1O_2\Sigma_0^{\frac{p-1}{4}}$. Die kleinsten p sind $119=16\cdot 7+1$ und $281=16\cdot 17+9$. $n=3$. Da $3^{\frac{p-1}{4}} \equiv 3^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ d. h. $\left(\frac{3}{p}\right)=1$, also $p=12h\pm 1$, und $p-1$ durch 4 teilbar ist, haben wir für p die beiden Formen $24h+1$ und $24h+13$. Folgende Möglichkeiten bestehen für die Wurzeln der Periodenkongruenz modulo 3: *1.* 0, 0, 0, −1. *2.* 1, 1, 1, −1.

[1] Vgl. WEBER, Algebra I, S. 634.

3. 0, 1, — 1, — 1. *4.* 0, 0, 1, 1. *5.* — 1, — 1, — 1, — 1, wenn nur (27) beachtet wird. Unter diesen sind die beiden letzten zu verwerfen. *4* führt auf $O_i^* = O_0 O_1 \Sigma_0^{-\frac{p-1}{2}}$ oder $O_i^* = O_0 O_2 \Sigma_0^{-\frac{p-1}{2}}$. In beiden Fällen gibt es eine $O_{i'}^*$, die mit O_i^* zusammengesetzt $O_0 O_1 O_2 O_3 = \Sigma_1 \ldots \Sigma_{p-1}$ gibt. Es ist nun $\{\Phi(\Sigma_1 \ldots \Sigma_{p-1})\} = H_3 p-1$, $\{\Phi(O_i^* O_{i'}^*)\}$ aber hat die Ordnung $3^{\frac{p-1}{2}}$. *5* ist auch wegen $H_3 p-1 = \{\Phi(\Sigma_1 \ldots \Sigma_{p-1})\}$ unmöglich. Aus $\Sigma \varrho_i \varrho_j$ schliesst man für $p = 24h + 1$: O^* vom Typus 1. O_0 oder 2. $O_0 O_1 O_2 O_3^{-1}$, für $p = 24h + 13$: O^* vom Typus 3. $O_0 O_1^{-1} O_2^{-1}$ oder $O_0 O_2^{-1} O_3^{-1}$. Die kleinsten Primzahlen der drei Kategorien sind:

1. $673 = 24.28 + 1 = 23^2 + 144$
2. $937 = 24 . 39 + 1 = 19^2 + 144 . 2^2$
3. 13.

Die Primzahlen der ersten und zweiten Kategorie sind notwendig in der Form $(12h_1 - 1)^2 + 144h_2^2$ bzw. $(12h_1 + 7)^2 + 144h_2^2$ darstellbar, worauf ich nicht eingehe.[1] Welche von den beiden Anordnungen $\alpha_0 : \alpha_1 : \alpha_2 : \alpha_3 = \begin{cases} 1 : -1 : -1 : 0 \\ 1 : 0 : -1 : -1 \end{cases}$ im dritten Falle die richtige ist, hängt von der Wahl der primitiven Wurzel γ ab. $\alpha_0 : \alpha_1 : \alpha_2 : \alpha_3 = 1 : -1 : 0 : -1$ ist aus ähnlichen Gründen wie oben *4.* und *5.* unmöglich.

Ist $z = 1$ d. h. $n - 1$ durch p teilbar, geht die Periodenkongruenz (14) in

$$\varrho^{p-1} + \varrho^{p-2} + \cdots 1 \equiv 0 \pmod{n}$$

über, und die Wurzeln sind $\varrho, \varrho^2, \varrho^3, \ldots, \varrho^{p-2}$, wenn ϱ zum Exponenten p modulo n gehört.

$$O^* = \Sigma_1^{\varrho^{1.i}} \Sigma_2^{\varrho^{2.i}} \ldots \Sigma_{p-1}^{\varrho^{(p-1)i}} . \Sigma_0 \text{ und } H_n = [1, O^*, O^{*2}, \ldots, O^{*n-1}].$$

Um den zur Gruppe H_{n^z} gehörigen Faktor F von $X^p - 1$

[1] Vgl. WEBER, Algebra I, S. 634.

modulo n zu finden, nachdem O^* bestimmt ist, sucht man $\alpha_0, \alpha_1, \ldots, \alpha_{\varkappa-1}$ derart, dass

$$(\alpha_0 + \alpha_1 X + \cdots \alpha_{\varkappa-1} X^{\varkappa-1} + X^\varkappa) O^* (X) \equiv 0 \text{ (modulis } n, X^p - 1),$$

was nur die Lösung linearer Kongruenzen erfordert.

m eine beliebige zu n teilerfremde Zahl.

Es genügt, wie schon oben[1] gezeigt ist, diejeningen H-Gruppen aufzusuchen, deren zugehörige Faktoren die in $X_{\varphi(m)}$ modulo n aufgehenden, irreduziblen Polynome sind. Ist $n^\varkappa \equiv 1 \pmod{m}$, so haben diese Gruppen $H_{n^\varkappa}$ die Ordnung $n^\varkappa$. Man kann ganz wie im vorhergehendan Falle von den Operationen O^* ausgehen. Die allgemeinste Form einer bei der Vertauschung $i' \equiv n\, i \pmod{m}$ invarianten Operation ist $O^* = O_0^{\alpha_0} O_1^{\alpha_1} \ldots O_s^{\alpha_s}$, wo O_i die Gestalt $\Sigma_a \Sigma_{a.n} \Sigma_{a.n^2} \ldots \Sigma_{a.n^{\varkappa i-1}}$ hat. Damit nun diese O^* zu

$$H_{n^{\varphi(m)}} \sim (\alpha_0 + \alpha_1 X + \cdots \alpha_{\varphi(m)-1} X^{\varphi(m)-1}) \frac{X^m - 1}{X_{\varphi(m)}}$$

gehöre, müssen die hinreichenden Bedingungen $\beta_i + \beta_{i+\frac{m}{p_1}} + \beta_{i+2.\frac{m}{p_1}} + \cdots \equiv 0 \bmod. n)$ für $i = 0, \ldots, \frac{m}{p_1} - 1$ und die analogen für $\frac{m}{p_3}, \frac{m}{p_3} \ldots$ erfüllt sein, wenn $O^* = \Pi \Sigma_i^{\beta_i}$. Dadurch sinkt die Zahl der unabhängigen α_i in $O_0^{\alpha_0} O_1^{\alpha_1} \ldots O_s^{\alpha_s}$ und muss genau $\frac{\varphi(m)}{\varkappa}$ werden, da die Zahl der in $H_{n^{\varphi(m)}}$ enthaltenen O^* genau $n^{\frac{\varphi(m)}{\varkappa}}$ ist. Ferner muss $\prod_{i=0}^{\varkappa-1} C^{-n^i} O^* C^{n^i} = O^{*\varrho}$, und daraus folgen ein System linearer Kongruenzen, wie oben (13), und eine Kongruenz vom Grade $\frac{\varphi(m)}{\varkappa}$, wie oben (14). Sind $\varrho_0, \varrho_1, \ldots, \varrho_{\frac{\varphi(m)}{\varkappa}-1}$ die Wurzeln dieser Kongruenz, so gilt

$$(15)' \qquad \alpha_0 : \alpha_1 : \ldots : \alpha_N = \varrho_{i_0} : \varrho_{i_1} : \ldots \varrho_{i_N},$$

[1] S. 11, 15.

wenn $\alpha_0, \alpha_1, \ldots, \alpha_N$ die Exponenten von $O_0, O_1, \ldots O_N$ sind, welche nur Σ_i enthalten, deren Index i zu m relativ prim ist, und $i_0, i_1, \ldots, i_N$ die Indices $0, 1, \ldots N$ in anderer Reihenfolge bedeuten. Σ_{-1} kommt in O_{i_0} vor. Geht $O_0 = \Sigma_1 \Sigma_n \ldots \Sigma_{n^{\varkappa-1}}$ durch die Vertauschung $i' \equiv g_j . i \pmod m$ in O_j über, so ist $X^{g_j} + X^{g_j . n} + \cdots + X^{g_j . n^{\varkappa-1}} = \varrho_{i_j}$ (modulis n, F), wo F derjenige modulo n irreduzible Faktor von $X_{\varphi(m)}$, ist, für welchen

$$X + X^n + \cdots X^{n^{\varkappa-1}} \equiv \varrho_{i_0} \text{ (modulis } n, F).$$

Ich nehme als Beispiel $m = 2^4$, $n = 7$, $\varkappa = 2$.

$$O^* = (\Sigma_1 \Sigma_7)^{\alpha_0} (\Sigma_3 \Sigma_5)^{\alpha_1} (\Sigma_9 \Sigma_{15})^{\alpha_2} (\Sigma_{11} \Sigma_{13})^{\alpha_3} (\Sigma_2 \Sigma_{14})^{\beta_1} (\Sigma_6 \Sigma_{10})^{\beta_2} (\Sigma_4 \Sigma_{12})^{\gamma} \Sigma_8^{\delta} \Sigma_0^{\varepsilon}$$

O^* ist in $H_{n^{\varphi(m)}}$ enthalten, wenn

$\alpha_0 + \alpha_2 \equiv 0 \pmod 7$; $\alpha_1 + \alpha_3 \equiv 0 \pmod 7$; $\beta_1 + \beta_2 \equiv 0 \pmod 7$; $2\gamma \equiv 0 \pmod 7$ und $\delta + \varepsilon \equiv 0 \pmod 7$. Es ist also

$$\alpha_2 \equiv -\alpha_0; \quad \alpha_3 \equiv -\alpha_1; \quad \beta_2 \equiv -\beta; \quad \gamma \equiv 0; \quad \varepsilon \equiv -\delta \pmod 7.$$

Aus $C^{-1} O^* C . C^{-7} O^* C^7 = O^{*\varrho}$ folgt nun

$$\begin{aligned} -\delta - \beta_1 &\equiv \varrho\, \alpha_0 \pmod 7 \\ \beta_1 &\equiv \varrho\, \alpha_1 \pmod 7 \\ \alpha_0 - \alpha_1 &\equiv \varrho\, \beta_1 \pmod 7 \\ 2\,\alpha_0 &\equiv \varrho\, \delta \pmod 7 \end{aligned}$$

und $\varrho^4 + 4\varrho^2 + 2 \equiv 0 \pmod 7$ mit den Wurzeln ± 1, ± 3. Man erhält für $\varrho = 1$ und $\alpha_2 = 1$ d. h. $\alpha_0 = -1$

$$\alpha_0 : \alpha_1 : \alpha_2 : \alpha_3 : \beta_1 : \beta_2 : \gamma : \delta : \varepsilon = -1 : 3 : 1 : -3 : 3 : -3 : 0 : 5 : 2.$$

Die übrigen Lösungen erhält man durch gleichzeitige zyklische Verschiebung von $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ und β_1, β_2.

Es sei ferner $m = p . q$ und $\varkappa = \frac{(p-1)(q-1)}{2}$. p und q sind zwei verschiedene Primzahlen. Ist $n^u \equiv 1 \pmod p$, $n^v \equiv 1 \pmod q$, so haben wir zwei wesentlich verschiedene Möglichkeiten:

1. $\mu = p-1;\ \nu = q-1.$

2. $\mu = \frac{p-1}{2};\ \nu = q-1.$

1. $O_1 = \Sigma_1 \Sigma_n \ldots \Sigma_{n^{\varkappa-1}},\ O_2 = \Sigma_a \Sigma_{a.n} \ldots \Sigma_{a.n^{\varkappa-1}},$
$S = \Sigma_q \Sigma_{n.q} \ldots \Sigma_{n^{p-2}.q} = \Sigma_q \Sigma_{2q} \ldots \Sigma_{(p-1)q},$
$T = \Sigma_p \Sigma_{n.p} \ldots \Sigma_{n^{q-2}.p} = \Sigma_p \ldots \Sigma_{(q-1)p}$ ($a \equiv n^i \pmod{p\,q}$,
$i = 0, 1, \ldots, \varkappa - 1.$)

Wir setzen nun

$$O^* = O_1^{\alpha} O_2^{\beta} . S^{\gamma} T^{\delta} \Sigma_0^{\varepsilon}.$$

Diese Operation ist in $H_{n^{\varphi(pq)}}$ enthalten, wenn
$\gamma \equiv -\frac{q-1}{2}(\alpha+\beta)$, $\delta \equiv -\frac{p-1}{2}(\alpha+\beta)$ und
$\varepsilon \equiv \frac{(p-1)(q-1)}{2}(\alpha+\beta)$, wie unmittelbar einleuchtet, falls man die Σ folgendermassen anordnet:

$$\begin{array}{llll} \Sigma_{0,0} & \Sigma_{1,0} & \ldots & \Sigma_{p-1,0}, \\ \Sigma_{0,1} & \Sigma_{1,1} & \ldots & \Sigma_{p-1,1}, \\ \cdot & \cdot & \cdot & \cdot \\ \Sigma_{0,q-1} & \Sigma_{1,q-1} & \ldots & \Sigma_{p-1,q-1}. \end{array}$$

$\Sigma_{i,j}$ steht für Σ_{iq+jp}.

Die Exponentensummen aller in derselben Zeile oder Kolonne stehenden Σ müssen $\equiv 0$ modulo n sein. Es ist

$$S = \Sigma_{1,0} \Sigma_{2,0} \ldots \Sigma_{p-1,0} \text{ und } T = \Sigma_{0,1} \Sigma_{0,2} \ldots \Sigma_{0,q-1}.$$

Nun haben wir

(30) $$\prod_{i=0}^{i=\varkappa-1} C^{-n^i} O^* C^{n^i} = O^{*\varrho_0},$$

(31) $$\prod C^{-an^i} O^* C^{an^i} = O^{*\varrho_1}$$ ($a \equiv n^i \pmod{p\,q}$ und relativ prim zu pq),

(32) $$\prod C^{-n^i} O_1^{\beta} O_2^{\alpha} S^{-\frac{q-1}{2}(\alpha+\beta)} T^{-\frac{p-1}{2}(\alpha+\beta)} \Sigma_0^{\frac{\varphi(pq)}{2}(\alpha+\beta)} C^{n^i} =$$
$$= (O_1^{\beta} O_2^{\alpha} \ldots)^{\varrho_1}.$$

(32) geht aus (31) durch die Vertauschung $i' = ai \pmod{pq}$ hervor. Man erhält nach einigen Rechnungen die zwei Bedingungen

$$(33) \qquad \alpha\varrho_0 + \beta\varrho_1 \equiv \frac{pq+1}{2}(\alpha+\beta) \pmod{n},$$

$$(34) \qquad \alpha\varrho_1 + \beta\varrho_1 \equiv \frac{-pq+1}{2}(\alpha+\beta) \pmod{n}.$$

Es genügt, die auf derselben Seite stehenden Operationen in (30) und (32) zusammenzusetzen. Ferner folgt aus (30) und (31) $\varrho_0 + \varrho_1 \equiv 1 \pmod{n}$. *Sind nun p und q beide von der Form $4h+3$, so kommt Σ_{-1} in O_1 vor und $\alpha:\beta \equiv \varrho_0:\varrho_1$, ist aber eine der Zahlen p, q von der Form $4h+1$, so wird $\alpha:\beta \equiv \varrho_1:\varrho_0$.* Dementsprechend erhalten wir

$$\varrho^2 - \varrho + \frac{1-pq}{4} \equiv 0 \pmod{n}$$

oder

$$\varrho^2 - \varrho + \frac{pq+1}{4} \equiv 0 \pmod{n}$$

für die Bestimmung von ϱ_0 und ϱ_1.

2. $\mu = \frac{p-1}{2}$, $\nu = q-1$. Ähnliche Berechnungen führen hier auf die für den Fall $m = p$, $\varkappa = \frac{p-1}{2}$ gefundenen Kongruenzen, wie ja zu erwarten ist, da die $H_{n^\varkappa}$ hier mit den $H_{n^{\mu,\nu}}$ zusammenfallen.[1]

Andere Darstellung der H-Gruppen.

Zu den bisher gefundenen Resultaten gelangt man auch auf eine andere Weise, wie wir jetzt zeigen wollen.

Es seien $0, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{p^\varkappa-1}$ die $p^\varkappa$ Zahlen eines GALOIS'schen Zahlkörpers:

$$\varepsilon = \alpha_1 i_1 + \alpha_2 i_2 + \cdots + \alpha_\varkappa i_\varkappa$$
$$(\alpha_1, \alpha_2, \ldots, \alpha_\varkappa = 0, 1, \ldots, p-1).$$

[1] S. 15.

Ferner gehöre die Zahl λ zum Exponenten m. m ist also ein Teiler von $p^\varkappa - 1$. Angenommen nun wir besässen irgend ein Mittel, wodurch die Zahlen ε derart auf die modulo p inkongruenten Zahlen $t: 0, 1, \ldots, p-1$ bezogen werden könnten, dass für $\varepsilon_1 \sim t_1$, $\varepsilon_2 \sim t_2$ auch $\varepsilon_1 + \varepsilon_2 \sim t_1 + t_2$, so ist offenbar, wenn die Primzahlordnung der Σ p ist,

$$H_{p^\varkappa} = [1, \Pi \Sigma_i^{\lambda^i \cdot \varepsilon_1}, \Pi \Sigma_i^{\lambda^i \cdot \varepsilon_2}, \ldots, \Pi \Sigma_i^{\lambda^i \varepsilon_{p^\varkappa - 1}}]$$

eine H-Gruppe. Dieselbe Gruppe gibt $[\Phi(O)]$ für

$$O = \Sigma_0^1 \Sigma_1^\lambda \Sigma_2^{\lambda^2} \ldots \Sigma_{m-1}^{\lambda^{m-1}},$$

da ja jede Zahl ε unter $\alpha_0 + \alpha_1 \lambda + \cdots + \alpha_{m-1} \lambda^{m-1}$ vorkommt. *Die gewünschte Beziehung zwischen den ε und t erhalten wir einfach dadurch, dass wir in allen ε statt $i_1, i_2, \ldots, i_\varkappa$ die Zahlen $t_1, t_2, t_\varkappa$ bzw. setzen.* Diese letzeren dürfen dabei natürlich nicht alle 0 sein aber sind sonst ganz beliebig. *Dasselbe erreichnen wir auch, wenn wir in einer Operation*, z. B. O, statt $i_1, i_2, \ldots, i_\varkappa$ *alle Kombinationen $t_1, t_2, \ldots, t_\varkappa$ setzen.* Es ist ja der Übergang von ε zu $\varepsilon \cdot \varepsilon'$ einer linearen, homogenen Substitution der α_i und somit einer ebensolchen der i gleichwertig.[1] *Die $\varphi(m)$ zu m gehörigen Zahlen λ liefern nur* $\frac{\varphi(m)}{\varkappa}$ *verschiedene H-Gruppen.* Denn λ und $\lambda^p, \lambda^{p^2}, \ldots, \lambda^{p^{\varkappa-1}}$ geben dieselbe Gruppe. Es läuft ja der Ersatz von λ durch λ^p in O darauf hinaus, dass wir $i_1^p, i_2^p, \ldots, i_\varkappa^p$ statt $i_1, i_2, \ldots, i_\varkappa$ schreiben und dann $i_1^p, i_2^p, \ldots, i_\varkappa^p$ durch $t_1, t_2, \ldots, t_\varkappa$ ersetzen.[2]

Da $1 + \lambda^{m_1} + \lambda^{2m_1} + \cdots + \lambda^{\left(\frac{m}{m_1}-1\right)m_1} = 0$ für jeden Teiler m_1 von m, so finden wir

$$\beta_i + \beta_{i+m_1} + \beta_{i+2m_1} + \cdots + \beta_{i+\left(\frac{m}{m_1}-1\right)m_1} \equiv 0 \pmod{p}$$

für $i = 0, 1, \ldots, m_1 - 1$ in jeder Operation $\Pi \Sigma_{ii}^{\beta}$ unserer H-Gruppe.

[1] Die Zahlen ε bilden bei Addition eine ABEL'sche $G_{p^\varkappa}$. Wir können somit ε der Substitution $z' \mid z + \varepsilon$ oder auch $z'_i \mid z_i + \alpha_i$ $(i = 1, 2, \ldots, \varkappa)$ entsprechen lassen. Durch Transformation mit $z' \mid \varepsilon' z$ geht $z' \mid z + \varepsilon$ in $z' \mid z + \varepsilon_1 \varepsilon'$ über, und somit muss $z'_i \mid z_i + \alpha_i$ in die $\varepsilon \cdot \varepsilon'$ entsprechende Substitution durch eine lineare homogene Transformation der α_i übergehen.

[2] Weil $i_1, i_2, \ldots, i_\varkappa$ und $i_1^p, i_2^p, \ldots, i_\varkappa^p$ gleichzeitig Basiszahlen sind.

Nehmen wir nun $\lambda^{\frac{m}{m_1}}$ statt λ und bilden $[\Phi(O)]$ für

$$O = \Sigma_0 \, \Sigma_1^{\lambda^{\frac{m}{m_1}}} \, \Sigma_2^{\lambda^{\frac{m}{m_1}\cdot 2}} \cdots \Sigma_{m-1}^{\lambda^{\frac{m}{m_1}(m-1)}},$$

so erhalten wir, wenn $p^{\varkappa_1} \equiv 1 \pmod{m_1}$,[1] eine $H_{p^{\varkappa_1}}$. Die Zahlen $\alpha_0 + \alpha_1 \lambda^{\frac{m}{m_1}} + \alpha_2 \lambda^{\frac{m}{m_1}\cdot 2} + \cdots + \alpha_{m-1} \lambda^{\frac{m}{m_1}(m-1)}$ erzeugen ja einen Zahlkörper der Ordnung $p^{\varkappa_1}$, und, wenn wir statt $i_1, i_2, \ldots, i_\varkappa$ in den Exponenten der Operation O alle Wertsysteme $t_1, t_2, \ldots, t_\varkappa$ schreiben, entstehen $p^{\varkappa_1}$ Operationen. Ferner ist $\lambda^{\frac{m}{m_1}(k\cdot m'+l)} = \lambda^{\frac{m}{m_1}\cdot l}$ und O ist von der Form $\Pi\left(\Sigma_i \, \Sigma_{i+m_1} \ldots \Sigma_{i+\left(\frac{m}{m_1}-1\right)m_1}\right)^{\gamma_i}$, wie wir oben gefunden haben.[2]

Wir haben ferner für alle Fälle gezeigt, wie man von einer H-Gruppe, deren zugehöriger, irreduzibler Faktor in $X_{\varphi(m)}$ aufgeht, zu entsprechenden H-Gruppen für jeden Teiler m_1 von m einfach dadurch herabsteigen kann, dass man nur diejenigen Σ_i behält, deren Indices durch $\frac{m}{m_1}$ teilbar sind, und Σ_i statt $\Sigma_{i\cdot\frac{m}{m_1}}$ schreibt. Dies folgt leicht aus der obigen Darstellung der H-Gruppen. Aus $O = \Pi \Sigma_i^{\lambda^i}$ geht ja $O' = \Pi \Sigma_{i\cdot\frac{m}{m_1}}^{\lambda^{\frac{m}{m_1}\cdot i}}$ oder nach Abänderung der Indizierung $O' = \prod_{i=0}^{m_1-1} \Sigma_i^{\lambda^{\frac{m}{m_1}\cdot i}}$ hervor. Dann wird $[\Phi(O')]$ eine $H_{p^{\varkappa_1}}$, wenn wir $i, i_1, \ldots, i_\varkappa$ durch $t_1, t_2, \ldots, t_\varkappa$ ersetzen, falls $p^{\varkappa_1} \equiv 1 \pmod{m_1}$.[1] Dasselbe erreichen wir durch Ersatz von $i_1, i_2, \ldots, i_\varkappa$ in O' mit allen Systemen $t_1, t_2, \ldots, t_\varkappa$, und dieser Ersatz endlich gibt dieselben Exponenten der $\Sigma_{i_{\frac{m}{m_1}}}$ wie die Substitution $t_1, t_2, \ldots, t_\varkappa$ in allen Operationen der $[\Phi(O)]$. Ist $\varkappa_1 < \varkappa$, müssen also mehrere Operationen der $H_{p^\varkappa}$ nach Entfernung aller Σ_i, deren Indices $\not\equiv 0 \left(\text{mod. } \frac{m}{m_1}\right)$, gleich ausfallen.

[1] $\varkappa_1$ Die kleinste Lösung.
[2] S. 11.

Über Folgen von gleichen Exponenten.

Die Operationen einer H_{p^z}, deren zugehöriger Faktor in $X_{\varphi(m)}$ aufgeht, können folgendermassen geordnet werden:

$$O_1, C^{-1} O_1 C, \ldots, C^{-(m-1)} O_1 C^{m-1}$$
$$O_2, C^{-1} O_2 C, \ldots, C^{-(m-1)} O_2 C^{m-1}$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$O_{\underbrace{p^z-1}_{m}}, C^{-1} O_{\underbrace{p^z-1}_{m}} C, \ldots, C^{-(m-1)} O_{\underbrace{p^z-1}_{m}} C^{m-1}.$$

In jeder Operation schreiben wir die Σ nach der natürlichen Reihenfolge der Indices und bezeichnen mit $F_\lambda^{(i)}$ eine Folge $(\Sigma_r \Sigma_{r+1} \ldots \Sigma_{r+\lambda-1})^i$, wenn die Exponenten von Σ_{r-1} und $\Sigma_{r+\lambda}$ von i verschieden sind. Insbesondere ist also $F_\lambda^{(0)}$ eine Lücke von λ konsekutiven Σ.[1] Man kann nun *die Anzahl* $A_\lambda^{(i)}$ *aller in* $O_1, O_2, \ldots O_{\underbrace{p^z-1}_{m}}$ *vorkommenden* $F_\lambda^{(i)}$ angeben und damit auch die (m-fache) Anzahl aller in den Operationen der Gruppe vorkommenden $F_\lambda^{(i)}$. Wir suchen zunächst *die Anzahl* $A_\lambda^{(0)}$ *der* $F_\lambda^{(0)}$ *in* $O_1, O_2, \ldots, O_{\underbrace{p^z-1}_{m}}$ und benutzen dabei einen Satz aus der Theorie der intransitiven Permutationsgruppen,[2] den wir für unseren besonderen Zweck so aussprechen können: Diejenigen Operationen irgend einer in $[\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}]$ enthaltenen Gruppe G_z (H-Gruppe oder nicht), welche mit von Null verschiedenen Exponenten

1. nur $\Sigma_r, \Sigma_{r+1}, \ldots, \Sigma_{r+\lambda-1}$

oder

2. nur $\Sigma_0, \Sigma_1, \ldots, \Sigma_{r-1}, \Sigma_{r+\lambda}, \Sigma_{r+\lambda+1}, \ldots$

enthalten, erzeugen zwei Gruppen:

1. G_{N_λ} von der Ordnung N_λ

und

2. $G_{N_{m-\lambda}}$ von der Ordnung $N_{m-\lambda}$.

Ferner geht G_N in eine $G_{N_\lambda'}$ über, wenn alle Σ_i ausser

[1] Dabei ist Σ_0 als auf Σ_{m-1} folgend anzusehen.
[2] BURNSIDE, Theory of groups, pag. 161.

$\Sigma_r, \Sigma_{r+1}, \ldots, \Sigma_{r+\lambda-1}$ überall gestrichen werden. *Es gilt dann*

$$\frac{N_\lambda}{N'_\lambda} = \frac{N_\lambda \cdot N_{m-\lambda}}{N}$$

oder

$$\frac{N}{N'_\lambda} = N_{m-\lambda}.$$

Die grösste mögliche $F^{(0)}_\lambda$ ist nun eine $F^{(0)}_{\varkappa-1}$, weil sonst die Ordnung der H-Gruppe $> p^\varkappa$ wäre. Wir betrachten $\Sigma_0, \Sigma_1, \ldots, \Sigma_{\lambda-1}$. Für jede $F^{(0)}_{\varkappa-1}$ in etwa O_1 gibt es eine Operation unter $O_1, C^{-1} O_1 C, \ldots, C^{-(m-1)} O_1 C^{m-1}$, welche nicht $\Sigma_0, \Sigma_1, \ldots, \Sigma_{\lambda-1}$ enthält. Die Zahl $N_{m-\lambda}$ wird also $1 + A^{(0)}_{\varkappa-1}$. Da, wie leicht ersichtlich, $N'_{\varkappa-1} = p^{\varkappa-1}$ ist, so haben wir

$$\frac{p^\varkappa}{p^{\varkappa-1}} = 1 + A^{(0)}_{\varkappa-1}, \quad A^{(0)}_{\varkappa-1} = p - 1.$$

Da wir nun bereits wissen, dass $F^{(0)}_{\varkappa-1}$ wirklich vorkommen (z. B. in $O \sim \frac{X^m - 1}{F}$, wenn F der zu $H_{p^\varkappa}$ gehörige Faktor ist), so muss $A^{(0)}_{\varkappa-1} = p - 1$ sein. Um dann $A^{(0)}_{\varkappa-2}$ zu finden bemerken wir, dass es für jede $F^{(0)}_{\varkappa-2}$ in etwa O_1 eine und für jede $F^{(0)}_{\varkappa-1}$ in O_1 zwei Operationen unter $O_1, C^{-1} O_1 C, \ldots, C^{-(m-1)} O_1 C^{m-1}$ gibt, welche $\Sigma_0, \Sigma_1, \ldots, \Sigma_{\lambda-1}$[1] nicht enthalten. Somit wird $N_{m-\lambda} = 1 + 2 A^{(0)}_{\varkappa-1} + A^{(0)}_{\varkappa-2}$ und, da $N'_{\varkappa-2} = p^{\varkappa-2}$ ist,

$$p^2 = 1 + 2(p-1) + A^{(0)}_{\varkappa-2}, \quad A^{(0)}_{\varkappa-2} = (p-1)^2.$$

Für $A^{(0)}_{\varkappa-3}$ erhalten wir genau in derselben Weise

$$p^3 = 1 + 3 A^{(0)}_{\varkappa-1} + 2 A^{(0)}_{\varkappa-2} + A^{(0)}_{\varkappa-3}, \quad A^{(0)}_{\varkappa-3} = p(p-1)^2.$$

Allgemein wird

$$A^{(0)}_{\varkappa-\lambda} = p^{\lambda-2}(p-1)^2 \text{ für } \lambda \geq 2,$$

wie man durch Induktion bestätigt. Es wird ja, die Richtigkeit der Behauptung für $A^{(0)}_{\varkappa-2}, A^{(0)}_{\varkappa-3}, \ldots, A^{(0)}_{\varkappa-\lambda}$ vorausgesetzt,

$$p^{\lambda+1} = 1 + (\lambda+1) A^{(0)}_{\varkappa-1} + \lambda \cdot A^{(0)}_{\varkappa-2} + \cdots + (i+2) A^{(0)}_{\varkappa-\lambda+i} + \cdots + 2 A^{(0)}_{\varkappa-\lambda} + A^{(0)}_{\varkappa-\lambda-1}$$

[1] $\lambda - 1 = \varkappa - 3$.

oder

$$A^{(0)}_{\varkappa-\lambda-1} = p^{\lambda+1} - [1 + (\lambda+1)(p-1) + \sum_{0}^{\lambda-2}(i+2)\,.\,p^{\lambda-(i+2)}(p-1)^2]$$

$$= p^{\lambda+1} - [1 + (\lambda+1)(p-1) + (p-1)^2 . p^{\lambda} \sum_{i=2}^{i=\lambda} i\, p^{-i}]$$

$$= p^{\lambda-1}(p-1)^2.$$

Wir haben ferner $A^{(1)}_{\lambda} = A^{(2)}_{\lambda} = \cdots = A^{(p-1)}_{\lambda}$, da ja eine $F^{(j)}_{\lambda}$ in eine $F^{(r)}_{\lambda}$ übergeht, wenn wir $O^r_1, O^r_2, \ldots, O^r_{p^{\varkappa}-1}$ statt $O_1, O_2, \ldots, O_{p^{\varkappa}-1}$ als Repräsentanten der $\frac{p^{\varkappa}-1}{m}$ Zeilen

$$O_i,\ C^{-1} O_i C,\ \ldots,\ C^{-(m-1)} O_i C^{(m-1)} \left(i = 1, 2, \ldots, \frac{p^{\varkappa}-1}{m}\right)$$

wählen. *Ausserdem gilt*

$$\sum_{i=0}^{i=p-1} A^{(i)}_{\lambda} = A^{(0)}_{\lambda-1}$$

oder

$$A^{(i)}_{\lambda} = \frac{1}{p-1}(A^{(0)}_{\lambda-1} - A^{(0)}_{\lambda}) = p^{\varkappa-\lambda-2}(p-1)^2 \text{ für } \lambda \leq \varkappa-2,\ i \neq 0.$$

Für $\lambda = \varkappa - 1$ *wird* $A^{(i)}_{\varkappa-1} = p-2$, *und endlich ist* $A^{(i)}_{\varkappa} = 1$ für $i = 1, 2, \ldots, p-1$.

Um dies einzusehen brauchen wir nur die Operationen unserer H-Gruppe nach folgendem Schema zu ordnen. Es stehen die $O(x)$ statt der O.

$$O_1(x),\ x\,O_1(x),\ \ldots,\ x^{m-1} O_1(x)$$
$$(x-1)\,O_1(x),\ (x-1)\,x\,O_1(x),\ \ldots,\ (x-1)\,x^{m-1} O_1(x)$$
$$(x-1)^2 O_1(x),\ (x-2)^2\,x\,O_1(x),\ \ldots,\ (x-1)^2\,x^{m-1} O_1(x)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(x-1)^r O_1(x),\ (x-1)^r\,x\,O_1(x),\ \ldots,\ (x-1)^r\,x^{m-1} O_1(x)$$
$$O'_2(x),\ x\,O'_2(x),\ \ldots,\ x^{m-1} O'_2(x)$$
$$(x-1)\,O'_2(x),\ (x-1)\,x\,O'_2(x),\ \ldots,\ (x-1)\,x^{m-1} O'(x)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(x-1)^r O'_2(x),\ (x-1)^r\,x\,O'_2(x),\ \ldots,\ (x-1)^r\,x^{m-1} O'_2(x) \text{ u. s. w.}$$

Erst $(x-1)^{r+1} O_1(x)$ kommt wieder in der ersten Zeile $O_1, C^{-1} O_1 C, \ldots, C^{-(m-1)} O_1 C^{m-1}$ vor.[1] Sind die Operationen mit der Zeile $(x-1)^r O_1(x) \ldots$ nicht erschöpft, nimmt man eine O'_2, welche nicht bereits vorkommt, und bildet $r+1$ neue Zeilen und so fort. Als Repräsentanten der Zeilen können wir natürlich wieder $O_1, O_2, \ldots, O_{\underbrace{p^z-1}_{m}}$ wählen. Nun ersieht man ohne weiteres, dass eine $F^{(0)}_{\lambda-1}$ immer eine $F^{(i)}_{\lambda}$ in dem vorhergehenden Repräsentanten voraussetzt, und dass umgekehrt jede $F^{(i)}_{\lambda}$ eine $F^{(0)}_{\lambda-1}$ in dem folgenden bewirkt.[2] Es erübrigt nur noch die Bestimmung von $A^{(i)}_1$. Diese Anzahl ermittelt man durch Berechnung der Anzahl aller übrigbleibenden Σ in $O_1, O_2, \ldots, O_{\underbrace{p^z-1}_{m}}$ nach Entfernung von allen $F^{(i)}_{z}, F^{(i)}_{z-1}, \ldots, F^{(i)}_{2}$ und $F^{(0)}_1$. So finden wir

$$A^{(1)}_1 + A^{(2)}_1 + \cdots + A^{(p-1)}_1 = (p-1) A^{(i)}_1 = p^z - 1 - \sum_{2}^{z} \lambda (A^{(0)}_\lambda + A^{(1)}_\lambda + \cdots +$$

$$+ A^{(p-1)}_\lambda) - A^{(0)}_1 = p^z - 1 - \sum_{2}^{z} \lambda \,.\, A^{(0)}_{\lambda-1} - A^{(0)}_1 = p^z - 1 - \sum_{1}^{z-1} A^{(0)}_\lambda -$$

$$- \sum_{2}^{z} (\lambda - 1) A^{(0)}_{\lambda-1} - A^{(0)}_1.$$

Nun ist aber $A^{(0)}_1 = p^{z-1} - 1 - \sum_{3}^{z} (\lambda - 1) A^{(0)}_{\lambda-1}$ nach dem oben gesagten, und also wird

$$(p-1) A^{(1)}_1 = p^z - 1 - (p^{z-1} - 1) - \sum_{1}^{z-1} A^{(0)}_\lambda - A^{(0)}_1 = p^z - p^{z-1} - (p-1) -$$

$$- \sum_{1}^{z-2} A^{(0)}_\lambda - A^{(0)}_1 = p^z - p^{z-1} - (p-1) - (p-1)^2 \sum_{0}^{z-3} p^i -$$

$$- (p-1)^2 . p^{z-3} = p^{z-1}(p-1) - p^{z-3}(p-1)^2 - p^{z-2}(p-1) =$$

$$= p^{z-3} (p-1)^3.$$

Also wird $A^{(1)}_1 = A^{(2)}_1 = \ldots = A^{(p-1)}_1 = p^{z-3}(p-1)^2 = A^{(0)}_1$.

Zusammenfassend haben wir also: Es ist für $\lambda \leq z-2$ $A^{(0)}_\lambda = A^{(1)}_\lambda = \cdots = A^{(p-1)}_\lambda = p^{z-\lambda-2}(p-1)^2$; $A^{(0)}_{z-1} = p-1$; $A^{(0)}_z = 0$; $A^{(1)}_{z-1} = A^{(2)}_{z-1} = A^{(p-1)}_{z-1} = p-2$ und $A^{(1)}_z = A^{(2)}_z = \cdots = A^{(p-1)}_z = 1$.

[1] Wäre etwa $(x-1)^{r+1} O_1(x) = (x-1)^i . x^j . O_1(x)$, käme $(x-1)^{r-i+1} O_1(x)$ schon in der ersten Zeile vor.

[2] Die O_i sind dabei nach dem obigen Schema in Zykeln von je $r+1$ geordnet.

Nichts hindert uns daran die Σ in den Operationen unseren H_{p^z} statt in der natürlichen Reihenfolge der Indices etwa in der Folge

$$\Sigma_0 \Sigma_k \Sigma_{2k} \dots \Sigma_{\binom{m}{k}-1)k}$$

zu schreiben, wenn k zu m relativ prim ist. Dann aber genügt es überall C^k statt C zu setzen, um zu genau denselben Schlüssen betreffs der $F_\lambda^{(i)}$ in den so geordneten Operationen zu gelangen. Das hätte man ja auch daraus folgern können, dass die besprochene Umordnung der Σ auf eine Substitution $i' = k \,.\, i$ der Indices hinausläuft, wodurch H_{p^z}, wie wir schon wissen, in eine H-Gruppe derselben Art[1] übergeht.

II. Die Ordnung der Σ_i eine Primzahlpotenz n^r. m nicht durch n teilbar.

In einer H-Gruppe, welche Operationen der Ordnungen $1, n, n^2, \dots, n^r$ enthält, ist der Inbegriff $\overset{(i)}{H}$ aller Operationen, deren Ordnung ein Teiler von n^i ist,[2] eine H-Gruppe. Für die Bestimmung der in $[\Sigma_0, \Sigma_1, \dots, \Sigma_{m-1}]$ enthaltenen H-Gruppen kann man ein rekurrentes Verfahren benutzen, indem man die $\overset{(i+1)}{H}$ aus den $\overset{(i)}{H}$ ableitet.

Von den $\overset{(1)}{H}$ wissen wir schon: Entsprechend der Zerlegung $F_1^{(1)} \,.\, F_2^{(1)} \dots F_s^{(1)}$ von $X^m - 1$ modulo n in irreduzible Faktoren gibt es s verschiedene $\overset{(1)}{H}$: $\overset{(1)}{H}_{n^{z_1}}, \overset{(1)}{H}_{n^{z_2}}, \dots, \overset{(1)}{H}_{n^{z_s}}$, die keine $\overset{(1)}{H}$ von niedriger Ordnung enthalten. Es ist

$$\left[\Sigma_0^{n^r-1}, \Sigma_1^{n^r-1}, \dots, \Sigma_{m-1}^{n^r-1}\right] = \overset{(1)}{H}_{n^{z_1}} \,.\, \overset{(1)}{H}_{n^{z_2}} \dots \overset{(1)}{H}_{n^{z_s}},$$

und jede $\overset{(1)}{H}$ lässt sich als Produkt einer Anzahl von diesen $\overset{(1)}{H}_{n^{z_j}}$ darstellen. Man kann $\overset{(1)}{H}_{n^{z_j}} = \left[\Phi(\overset{(1)}{O}_j)\right]$ für

[1] deren zugehöriger Faktor in $X_{g(m)}$ aufgeht.

[2] i möglichst klein.

$$\overset{(1)}{O_j} \sim n^{r-1} \cdot \frac{X^m - 1}{\overset{(1)}{F_j}}$$

setzen.

Es gibt Symbole Φ, die zu allen $\overset{(1)}{H^j}$ mit Ausnahme einer einzigen gehören.

Wir gehen nun zu den $\overset{(2)}{H}$ über und suchen über $\overset{(1)}{H}_{n^{z_j}}$ eine $\overset{(2)}{H}_{n^{2z_j}}$ zu konstruieren, welche $\overset{(1)}{H}_{n^{z_j}}$ als einzige $\overset{(1)}{H}$ enthält. Zu dem Zwecke suchen wir ein Polynom

$$O(X) = n^{r-2} \cdot \frac{X^m - 1}{\overset{(1)}{F_j}} + n^{r-1} \cdot Z$$

derart zu bestimmen, dass

$$\overset{(1)}{F_j} \cdot O(X) \equiv 0 \left(\text{modulis } n^r, n^{r-1} \cdot \frac{X^m - 1}{\overset{(1)}{F_j}} \right) \tag{35}$$

ist. $\dfrac{X^m - 1}{\overset{(1)}{F_j}}$ ist modulo n zu nehmen, und es sei

$$\frac{X^m - 1}{\overset{(1)}{F_j}} \cdot \overset{(1)}{F_j} \equiv n \cdot Y \text{ (modulis } n^2, X^m - 1). \tag{36}$$

Da $\dfrac{X^m - 1}{\overset{(1)}{F_j}}$ und $\overset{(1)}{F_j}$ modulo n teilerfremd sind, ist es immer möglich G_1 und G_2 so zu wählen, dass

$$1 \equiv G_1 \cdot \frac{X^m - 1}{\overset{(1)}{F_j}} + G_2 \cdot \overset{(1)}{F_j} \text{(mod. } n)$$

und

$$n^{r-1} \cdot Y \equiv n^{r-1} \cdot Y \cdot G_1 \cdot \frac{X^m - 1}{\overset{(1)}{F_j}} + n^{r-1} \cdot Y \cdot G_2 \cdot \overset{(1)}{F_j} \text{(mod. } n^r) \tag{37}$$

wird. Nun ist

$$\overset{(1)}{F_j}.O(X) \equiv n^{r-1}(Y + \overset{(1)}{F_j}.Z) \text{ (modulis } n^r, X^m - 1)$$

nach (36) oder nach (37)

$$\overset{(1)}{F_j}.O(X) \sim n^{r-1}\left[Y.G_1 \cdot \frac{X^m-1}{\overset{(1)}{F_j}} + \right.$$

$$\left. + (Z + Y.G_2).\overset{(1)}{F_j}\right] \text{(modulis } n^r, X^m - 1),$$

und es genügt $Z \ldots - Y.G_2$ (mod. n) zu setzen um (35) zu erfüllen.

$\overset{(2)}{H}_{n^{2\varkappa_j}} = [\Phi(O)]$ für

$$O \sim n^{r-2}\left[\frac{X^m-1}{\overset{(1)}{F_j}} - n.Y.G_2\right]$$

ist dann eine $\overset{(2)}{H}$ *der verlangten Art.* Zunächst enthält $\overset{(2)}{H}_{n^{2\varkappa_j}}$ die Gruppe $\overset{(1)}{H}_{n^{\varkappa_j}}$, da ja $\overset{(1)}{H}_{n^{\varkappa_j}} = [\Phi(O^n)]$. Ferner enthält $[\Phi(O)]$ keine andere Operationen n:ter Ordnung. (35) besagt nämlich, dass $\Phi(O)$ in $\overset{(1)}{H}_{n^{\varkappa_j}}$ für alle Φ, deren entsprechende Polynome von der Form $\overset{(1)}{F_j}.G(X)$ sind enthalten ist. Enthält somit $[\Phi(O)]$ eine Operation n:ter Ordnung, die nicht in $\overset{(1)}{H}_{n^{\varkappa_j}}$ vorkommt, so muss dies auch der Fall sein für eine $\Phi'(O)$, wo das Φ' entsprechende Polynom Φ'_x nicht den Grad $\varkappa_j$ erreicht.[1] Ist aber $\Phi'(O)$ von der n:ten Ordnung, muss $\Phi'(O^n) = 1$, und dies ist unmöglich, weil Φ'_x nicht modulo n durch $\overset{(1)}{F}_{n^{\varkappa_j}}$ teilbar ist. Nun schliessen wir leicht, dass die Ordnung der Gruppe $[\Phi(O)]$ $n^{2\varkappa_j}$ ist. $\overset{(1)}{H} = [\Phi(O^n)] = \overset{(1)}{H}_{\varkappa_j}$ ist mit $[\Phi(O)]$ $1{:}n^{\varkappa_j}$-stufig isomorph, da der Inbegriff $\overset{(1)}{H}$ aller Operationen n:ter Ordnung in $[\Phi(O)]$ die Ordnung $n^{\varkappa_j}$ hat. $[\Phi(O)]$ hat also die Ordnung $n^{\varkappa_j}.n^{\varkappa_j} = n^{2\varkappa_j}$. *Es ist auch leicht ersichtlich,*

[1] und alle Koeffizienten nicht durch p teilbar sind.

dass $\overset{(2)}{H}_{n^{2\varkappa_j}}$ *keine andere* $\overset{(2)}{H}$ *enthält.* Denn die darin enthaltenen $\overset{(1)}{H}$ und $\overset{(1)}{H}$ müssen notwendig mit $\overset{(1)}{H}_{n^{\varkappa_j}}$ zusammenfallen, und die Ordnung wird dem Isomorphismus zufolge $n^{2\varkappa_j}$.

O ist durch (35) nur bis auf Operationen in $\overset{(1)}{H}_{n^{\varkappa_j}}$ bestimmt, und dies benutzen wir um O auf eine besondere Form $\overset{(2)}{O}$ zu bringen. Wir fügen nämlich geeignete Operationen aus $\overset{(1)}{H}_{n^{\varkappa_j}}$ derart zu O hinzu, dass ein $\overset{(2)}{O}(X) = n^{r-2}(\alpha_0 + \alpha_1 X + \cdots + X^{m-\varkappa_j})$ der Operation $\overset{(2)}{O}$ entspricht. Dann ist $X^m - 1$ modulo n^2 durch $\overset{(2)}{O}(X)$ teilbar und wir setzen $\overset{(2)}{O}(X) = n^{r-2} \cdot \frac{X^m - 1}{\overset{(2)}{F}_j}$; $\overset{(2)}{O}(X) \cdot \overset{(2)}{F}_j \equiv 0$ (modulis n^r, $X^m - 1$). Die Gruppe $\left[\Phi(\overset{(2)}{O})\right]$ hat ja die Ordnung $n^{2\varkappa_j}$ und $\overset{(2)}{O}$, $C^{-1}\overset{(2)}{O}C, \ldots,$ $C^{-(\varkappa_j-1)}\overset{(2)}{O}C^{\varkappa_j-1}$ ist eine Basis. Somit muss

$$X^{\varkappa_j} \cdot \overset{(2)}{O}(X) \equiv \overset{(2)}{O}(X)\left[\beta_0 + \cdots + \beta_{\varkappa_j-1} \cdot X^{\varkappa_j-1}\right] \text{(modulis } n^r, X^m - 1)$$

sein, und da $n^{r-2}X^m$ wirklich in $X^{\varkappa_j}\overset{(2)}{O}(X)$ vorkommt, ist dies nur möglich, wenn $X^m - 1$ modulo n^r durch $\overset{(2)}{O}(X)$ teilbar ist. So erhalten wir die Gruppen

$$\overset{(2)}{H}_{n^{2\varkappa_1}}, \overset{(2)}{H}_{n^{2\varkappa_2}}, \ldots, \overset{(2)}{H}_{n^{2\varkappa_s}}$$

und die entsprechenden Polynome

$$\overset{(2)}{F}_1, \overset{(2)}{F}_2, \ldots, \overset{(2)}{F}_s$$

Es ist $\left[\Sigma_0 n^{r-2}, \Sigma_1 n^{r-2}, \ldots, \Sigma_{m-1} n^{r-2}\right] = \overset{(2)}{H}_{n^{2\varkappa_1}} \cdot \overset{(2)}{H}_{n^{2\varkappa_2}} \cdot \ldots \cdot \overset{(2)}{H}_{n^{2\varkappa_s}}$.

Denn $\varkappa_1 + \varkappa_2 + \cdots + \varkappa_s = m$ und $2\varkappa_1 + 2\varkappa_2 + \cdots + 2\varkappa_s = 2m$. Eine Identität $1 = O_1 \cdot O_2 \ldots O_s$ kann aber nicht gelten, wie

man sich durch Erheben zur n:ten Potenz überzeugt. Somit erreicht die Ordnung der rechtsstehenden Gruppe wirklich $2m$.

$$\textit{Ferner ist } X^m - 1 \equiv \overset{(2)}{F_1} \cdot \overset{(2)}{F_2} \cdots \overset{(2)}{F_s} (\mathrm{mod.}\, n^2).$$

Das $\overset{(2)}{F_1} \cdot \overset{(2)}{F_2} \cdots \overset{(2)}{F_s}$ entsprechende Symbol gehört ja zu allen $\overset{(2)}{H_j}$, und da $\overset{(2)}{F_1} \cdot \overset{(2)}{F_2} \cdot \overset{(2)}{F_s}$ X^m enthält, ist dies nur möglich, wenn

$$\overset{(2)}{F_1} \cdot \overset{(2)}{F_2} \cdots \overset{(2)}{F_s} \equiv X^m - 1 \,(\mathrm{mod.}\, n^2) \text{ ist.}$$

$\Phi_1 \sim \dfrac{X^m - 1}{\overset{(2)}{F_1}}$ *gehört zu allen* $\overset{(2)}{H_{n^{2z_j}}}$ *mit Ausnahme von* $\overset{(2)}{H_{n^{2z_1}}}$ *und* $\Phi_1(O_1)$ *ist von der* n^2*:ten Ordnung,* wenn O_1 von dieser Ordnung ist. Somit ist $[\Phi\{\Phi_1(O_1)\}]$ mit $\overset{(2)}{H_{n^{2z_1}}}$ identisch. *Schliesslich ist jede* $\overset{(2)}{H}$ *als das direkte Produkt einer Anzahl* $\overset{(2)}{H_{n^{2z_j}}}$ *und* $\overset{(1)}{H_{n^{z_j}}}$ *darstellbar.* Man braucht ja nur eine Operation in $\overset{(2)}{H}$ von der n^2:ten Ordnung auszuwählen, welche, in der Form $O_1 \cdot O_2 \cdot O_3 \ldots$ geschrieben, Operationen O_i aus möglichst vielen $\overset{(2}{H_{n^{2z_j}}}$ und $\overset{(1)}{H_{n^{z_j}}}$ enthält. $\overset{(2)}{H}$ ist dann das Produkt dieser $\overset{(2)}{H_{n^{2z}}}$ und $\overset{(1)}{H_{n^{z_j}}}$.

Wir wollen nun annehmen, dass die analogen Tatsachen noch für die Ordnungen n^3, $n^4, \ldots,$ n^{i-1} gelten und führen dann den Beweis auch für die Ordnung n^i. Es sei also:

I. $$X^m - 1 \equiv \overset{(i-1)}{F_1} \cdot \overset{(i-1)}{F_2} \cdots \overset{(i-1)}{F_s} (\mathrm{mod.}\, n^{i-1}),$$

II. $\overset{(i-1)}{H}_{n^{(i-1)z_j}} = [\Phi(O)]$ für $O \sim n^{r-(i-1)} \cdot \dfrac{X^m - 1}{\overset{(i-1)}{F_j}}$ enthält als $\overset{(i-1)}{F_j} \equiv \overset{(1)}{F_j} (\mathrm{mod.}\, n)$. Der Koeffizient von X^{z_j} ist $= 1$ gewählt.

einzige $\overset{(1)}{H}$, $\overset{(2)}{H}, \ldots$ die analogen $\overset{(1)}{H_{n^{z_j}}}$, $\overset{(2)}{H_{n^{2z_j}}}, \ldots$

III. Jede Operation der Ordnung n^{i-1} kann aus Operationen in den $\overset{(i-1)}{H}_{n^{(i-1)\varkappa_j}}$ zusammengesetzt werden, und

IV. jede $\overset{(i-1)}{H}$ ist das Produkt einer Anzahl $\overset{(i-1)}{H}_{n^{(i-1)\varkappa_j}}$, $\overset{(i-2)}{H}_{n^{(i-2)\varkappa_j}}, \ldots$

Nun konstruieren wir über $\overset{(i-1)}{H}_{n^{(i-1)\varkappa_j}}$ eine $\overset{(i)}{H}_{n^{i}\cdot\varkappa_j}$, welche diese $\overset{(i-1)}{H}_{n^{(i-1)\varkappa_j}}$ als einzige $\overset{(i-1)}{H}$ enthält. Wie oben gehen wir von

$$O(X) = n^{r-i}\left[\frac{X^m - 1}{\overset{(i-1)}{F_j}} + n^{i-1}\cdot Z\right]$$

aus und bestimmen Z derart, dass $\Phi(O)\sim O(X)\,.\,\overset{(i-1)}{F_j}$ in $\overset{(i-1)}{H}_{n^{(i-1)\varkappa_j}}$ enthalten ist, d. h.

$$O(X)\,.\,\overset{(i-1)}{F_j} \equiv 0 \left(\text{modulis } n^r, \frac{X^m - 1}{\overset{(i-1)}{F_j}}\right) \tag{38}$$

Dies geschieht ganz in derselben Weise wie oben, und wir kommen dann durch Hinzufügung von Operationen in $\overset{(i-1)}{H}_{n^{(i-1)\varkappa_i}}$ zu der Operation $\overset{(i)}{O}$:

$$\overset{(i)}{O} \sim n^{r-i}\left[\alpha'_0 + \alpha'_1 X + \cdots + X^{m-\varkappa_i}\right]$$

Die Gruppe $[\Phi(O)]$ *hat die verlangten Eigenschaften.* Sie enthält

$$\overset{(i-1)}{H}_{n^{(i-1)\varkappa_j}} = [\Phi(O^n)].$$

Ferner enthält sie keine andere Operationen n^{i-1}:ter Ordnung als die in $\overset{(i-1)}{H}_{n^{(i-1)\varkappa_j}}$ vorkommenden. Denn ist $\Phi'(O)$ eine solche Operation, so kann man nach (38) Φ'_x vom Grade $\varkappa' < \varkappa_j$ annehmen. Dann muss aber $\Phi'(O^{n^{i-1}}) = 1$, was unmöglich ist.[1] Die Gruppe $[\Phi(O^{n^{i-1}})]$ ist mit $\overset{(1)}{H}_{n^{\varkappa_j}}$ identisch.

[1] Alle Koeffizienten in $\Phi' x$ sind nicht durch p teilbar.

Da $[\Phi(O)]$ und $[\Phi(O^{n^{i-1}})]$ $n^{(i-1)z_j}$: 1-stufig isomorph sind, *muss* $[\Phi(O)]$ *die Ordnung* $n^{i \cdot z_j}$ *haben.* $[\Phi(O)]$ *kann keine kleinere* $\overset{(i)}{H}$ *enthalten.* Denn die darin vorkommende $\overset{(i-1)}{H}$ muss nach der Voraussetzung $\overset{(i-1)}{H}_{n^{(i-1)z_j}}$ sein und die $\overset{(1)}{H}$, welche entsteht, wenn man jede Operation zur n^{i-1}:ten Potenz erhebt, muss mit $\overset{(1)}{H}_{n^{z_j}}$ identisch sein. Die Ordnung ist also $n^{i \cdot z_j}$. Man schliesst ferner, dass $\overset{(i)}{H}_{n^{iz_j}} = \left[\overset{(i)}{\Phi(O)}\right]$, und daraus, dass $X^m - 1$ modulo n^r durch $\overset{(i)}{O}(X)$ teilbar ist. Wir setzen $\overset{(i)}{H}_{n^{iz_j}} = [\overset{(i)}{\Phi(O)}$ für $\overset{(i)}{O} \sim n^{r-i} \cdot \dfrac{X^m - 1}{\overset{(i)}{F_j}}$. Es ist dann

$$\left[\Sigma_0 n^{r-i}, \Sigma_1 n^{r-i}, \ldots, \Sigma_{m-1}^{n^{r-i}}\right] = \overset{(i)}{H}_{n^{iz_1}} \ldots \overset{(i)}{H}_{n^{i \cdot z_s}},$$

was aus der entsprechenden Annahme für $i-1$ folgt. Dass $\overset{(i)}{F_1} \cdot \overset{(i)}{F_2} \ldots \overset{(i)}{F_s} \equiv X^m - 1$ modulo n^i sein muss, folgt wie oben. $\Phi_1 \sim \dfrac{X^m - 1}{\overset{(i)}{F_1}}$ gehört zu allen $\overset{(i)}{H}_{n^{i \cdot z_j}}$ mit Ausnahme von $\overset{(i)}{H}_{n^{i \cdot z_1}}$, und es ist $\Phi_1(O_1)$ von der n^i:ten Ordnung, wenn O_1 diese Ordnung hat.[1] Somit ist

$$[\Phi(\Phi_1(O_1))] = \overset{(i)}{H}_{n^{iz_j}}.$$

Schliesslich ist es dann klar, wie man durch Anwendung dieser Symbole jede $\overset{(i)}{H}$ in das Produkt einer Anzahl $\overset{(1)}{H}_{n^{z_j}}$, $\overset{(2)}{H}_{n^{2z_j}}, \ldots,$ $\overset{(i)}{H}_{n^{iz_j}}$ auflösen kann. Dass $\overset{(i)}{H}_{n^{iz_1}}$ keine andere $\overset{(1)}{H}_{n^{z_j}}$, $\overset{(2)}{H}_{n^{2z_j}}, \ldots,$ $\overset{(i-1)}{H}_{n^{(i-1)z_j}}$ als $\overset{(1)}{H}_{n^{z_1}}$, $\overset{(2)}{H}_{n^{2z_1}}, \ldots,$ $\overset{(i-1)}{H}_{n^{(i-1)z_1}}$ enthalten kann, folgt daraus, dass die $\overset{(i)}{H}_{n^{iz_i}}$ keine gemeinschaftlichen Operationen ausser der Einheit besitzen. Somit sind die Eigenschaften der $\overset{(i)}{H}$ als denen der $\overset{(i-1)}{H}$ völlig analog erwiesen, und wir können sukzessiv zu beliebig hohen Ordnungen aufsteigen.

[1] Sonst wäre $\Phi_1(O_1 n^{i-1}) = 1$, was unmöglich ist.

Haben wir schliesslich die $\overset{(r)}{H}_{n^{rz}j}$ gefunden, so können wir jede in $[\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}]$ enthaltene H-Gruppe angeben und zwar in der Form

$$\prod_{j_1} \overset{(1)}{H}_{n^{z_{j_1}}} \cdot \prod_{j_2} \overset{(2)}{H}_{n^{2z_{j_2}}} \cdot \ldots \cdot \prod_{j_r} \overset{(r)}{H}_{n^{iz_{j_r}}} \text{ oder}$$

auch

$$\prod_{j} \left[\overset{(r)}{H}_{n^{r} \cdot z_j}\right]^{n^{a_j}},$$

wenn

$\left[\overset{(r)}{H}_{n^{i} \cdot z_j}\right]^{n^{a_j}}$ die Gruppe bezeichnet, welche aus $\overset{(i)}{H}_{n^{iz_j}}$ hervorgeht, wenn jede Operation zur n^{z_j}:ten Potenz erhoben wird. *Die Anzahl der H-Gruppen ist* $(r+1)^s$.

Man kann ferner bemerken, dass es in jeder H-Gruppe Operationen O gibt für welche $H = [\Phi(O)]$. $O(X)$ kann immer in der Form $\sum_{j=1}^{j=r} p^{a_j} \cdot \frac{X^m - 1}{\overset{(r)}{F}_j}$ angenommen werden. Es folgt dann leicht, *dass* $\Phi_x = \sum_{j=1}^{j=r} p^{r-a_j} \frac{X^m - 1}{\overset{(r)}{F}_j}$ *ein Polynom ist, dessen entsprechendes Symbol zur Gruppe H gehört,* und dass alle solche Symbole den Polynomen $G(X) \cdot \Phi_x$ entsprechen. Als Beispiel der hier besprochenen Zerlegung von $X^m - 1$ modulo $n, n^2, n^3, \ldots$ diene

$$\begin{aligned} X^7 - 1 &\equiv (X+1)(X^3+X^2+1)(X^3+X+1) \pmod 2 \\ &\equiv (X+3)(X^3+3X^2+2X+3)(X^3+2X^2+X+3) \pmod 4 \\ &\equiv (X+7)(X^3+3X^2+2X+7)(X^3+6X^2+5X+7) \pmod 8 \\ &\equiv (X+15)(X^3+11X^2+10X+15)(X^3+6X^2+5X+15) \\ &\qquad \pmod{16}. \end{aligned}$$

III. Die Ordnung der Σ_i eine Primzahlpotenz n^i; $m = n^r \cdot m$.

Die Einfachheit der Verhältnisse im vorhergehenden Falle rührt wesentlich davon her, dass $X^m - 1$ modulo n in *ver-*

schiedene, irreduzible Faktoren zerfällt. Daraus folgt dann eine Zerlegung derselben Art von $X^m - 1$ modulo $n^2, n^3, \ldots$ u. s. w., und die H-Gruppen sind durch diese Zerlegung sofort gegeben. Ist aber m durch n teilbar: $m = n^r \cdot m_1$, wird $X^m - 1 \equiv (X^{m_1} - 1)^{n^r} \pmod{n}$, und es gibt nicht mehr eine eindeutige Zerlegung von $F^m - 1$ modulo $n^2, n^3, \ldots$ Nimmt man zum Beispiele in einer $\overset{(2)}{H}$ die Gruppen $\overset{(1)}{H}$ und $[\overset{(2)}{H}]^{n_1}$ als gegeben an, so gibt es bald eine bald keine oder mehrere $\overset{(2)}{H}$, welche die Bedingungen erfüllen.

Im Falle $m = n \cdot m_1$, wo m_1 zu n teilerfremd ist, gelingt die Bestimmung der in $[\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}]$ enthaltenen $\overset{(i)}{H}$-Gruppen am einfachsten. Wir schreiben jetzt p statt n und m statt m_1. $X^{pm} - 1$ ist durch $X^m - 1$ teilbar. $X^m - 1$ zerfällt aber modulo p^i in $\overset{(i)}{F}_1(X) \cdot \overset{(i)}{F}_2(X) \ldots \overset{(i)}{F}_s(X)$, wie schon oben gezeigt. Dementsprechend zerfällt $X^{pm} - 1$ modulo p^i in $\overset{(i)}{F}_1(X^p) \cdot \overset{(i)}{F}(X^p) \ldots \overset{(i)}{F}_s(X^p)$:

$$X^{pm} - 1 \equiv \overset{(i)}{F}_1(X^p) \cdot \overset{(i)}{F}_2(X^p) \ldots \overset{(i)}{F}_s(X^p) \pmod{p^i}.$$

Da $\overset{(i)}{F}_j(X^p) \equiv [\overset{(i)}{F}_j(X)]^p \pmod{p}$, folgt, dass $\overset{(i)}{F}_1(X^p), \overset{(i)}{F}_2(X^p), \ldots, \overset{(i)}{F}_r(X^p)$ modulo $p, p^2, \ldots, p^i$ relativ prim sind. Ferner ist $\overset{(i)}{F}_j(X^p)$ modulo p^i durch $\overset{(i)}{F}_j(X)$ teilbar, weil $\overset{(i)}{F}_j(X)$ in $X^m - 1$ und somit in $X^{pm} - 1$ modulo p^i aufgeht und schon modulo p nur in $\overset{(i)}{F}_j(X^p)$ aufgehen kann.

Der Zerlegung $\overset{(i)}{F}_1(X^p) \ldots \overset{(i)}{F}_s(X^p)$ von $X^{pm} - 1$ entsprechend können wir $[\Sigma_0, \Sigma_1, \ldots, \Sigma_{pm-1}]$ als das Produkt $\overset{(i)}{H}_1 \cdot \overset{(i)}{H}_2 \ldots \overset{(i)}{H}_s$ auffassen, wo $\overset{(i)}{H}_j = [\Phi(\overset{(i)}{O}_j)]$ und $\overset{(i)}{O}_j \sim \frac{X^{pm} - 1}{\overset{(i)}{F}_j(X^p)}$. Es ist ferner jede in $[\Sigma_0, \Sigma_1, \ldots, \Sigma_{pm-1}]$ enthaltene H-Gruppe das direkte Produkt von Untergruppen der $\overset{(i)}{H}_j$, welche selbst H-Gruppen sind. Dies folgt daraus, dass die $\overset{(i)}{F}_j(X^p)$ modulo p relativ prim sind. Es genügt also die Untergruppen von $\overset{(i)}{H}_j$ zu

[1] S. 45.

bestimmen, welche H-Gruppen sind. Dabei können wir uns ausserdem auf eine derjenigen $\overset{(i)}{H}_j$ beschränken, welche den Faktoren von $X_{\varphi(m)}$ entsprechen.

Es seien also $\overset{(i)}{F}_1(X), \overset{(i)}{F}_2(X), \ldots, \overset{(i)}{F}_{\varphi(m)}(X)$ die Faktoren modulo p^i von $X_{\varphi(m)}$ und $\overset{(i)}{H}_1, \overset{(i)}{H}_2, \ldots$ die zu $\overset{(i)}{F}_1(X^p), \overset{(i)}{F}_2(X^p), \ldots$ gehörenden H-Gruppen. Diese sind isomorpf und enthalten alle gleich viele H-Gruppen.

Der Bestimmung dieser Gruppen schicke ich folgende Bemerkung voraus:

$\dfrac{\overset{(i)}{F}_1(X^p)}{\overset{(i)}{F}_1(X)}$ *ist nicht modulo* p^2 *durch* $\overset{(i)}{F}_1(X)$ *teilbar.* Dann wäre ja $X_{\varphi(pm)} = \Pi \dfrac{\overset{(i)}{F}(X^p)}{\overset{(i)}{F}(X)}$ durch $X_{\varphi(m)} = \Pi \overset{(i)}{F}(X)$ modulo p^2 teilbar, und alle Operationen der Gruppe $[\Phi(O_1)]$ für

$$O_1 \sim \frac{X^{pm}-1}{X_{\varphi(m)}}$$

müssten in der Gruppe $[\Phi(O_2)]$ für

$$O_2 \sim \frac{X^{pm}-1}{X_{\varphi(pm)}}$$

enthalten sein. Die Σ sind von der Ordnung p^2. Da alle Operationen der ersten Gruppe von der Form

$$\prod_i (\Sigma_i \Sigma_{i+m} \ldots \Sigma_{i+(p-1)m})^{\alpha_i}$$

sind, diejenigen der zweiten aber von der Form $\prod_i \Sigma_i^{\beta_i}$ mit den Bedingungen

$\beta_i + \beta_{i+m} + \cdots + \beta_{i+(p-1)m} \equiv 0 \pmod{p^2}$, $(i = 0, 1, \ldots, m-1)$, so können nicht alle $\Phi(O_1)$ in $[\Phi(O_2)]$ vorkommen.[1]

Erhebt man alle Operationen einer in $\overset{(i)}{H}_1$ enthaltenen $\overset{(i)}{H}$

[1] Vgl. oben S. 11, 12.

zur p^{i-1}:ten Potenz, so geht eine $\overset{(i)}{H}$ hervor, welche, als in $\overset{(i)}{H}_1$ enthalten, von der Form $[\Phi(O)]$, für

$$O \sim p^{i-1} \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot [\overset{(i)}{F}_1(X)]^j,$$

sein muss. Also enthält unsere H gewiss eine H-Gruppe $[\Phi(O')]$ für

$$O' \sim \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot \{[\overset{(i)}{F}_1(X)]^j + p^r . G(X)\},$$

wo $G(X)$ ein beliebiges Polynom ist, dessen Koeffizienten nur nicht alle durch p teilbar sind.

Nun zeigen wir:

Eine in $\overset{(i)}{H}_1$ *enthaltene H-Gruppe* $[\Phi(O)]$ *mit*

$$O \sim \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \{[\overset{(i)}{F}_1(X)]^j + p^r . G(X)\}$$

enthält für $j < p-1$ *immer*

$$O' \sim p \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot \overset{(i)}{F}_1(X)$$

und

$$O'' \sim p^{r'+1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)}, \quad (r' \geq r)$$

woraus dann folgt, dass man, ohne die H-Gruppe zu ändern, O durch

$$\bar{O} . \sim \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \{[\overset{(i)}{F}_1(X)]^j + p^{r'} (\alpha_0 + \alpha_1 X + \cdots \alpha_{\varkappa-1} X^{\varkappa-1})\}$$

$$(\alpha_0, \alpha_1, \ldots \alpha_{\varkappa-1} = 0, 1, \ldots, p-1)$$

ersetzen kann. Damit ist also eine gewisse Normierung der $\overset{(i)}{H}$ gewonnen. In $[\Phi(O)]$ kommt nun zunächst

$$\bar{O}' \sim \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot \{[\overset{(i)}{F}_1(X)]^p + p^r \cdot [\overset{(i)}{F}_1(X)]^{p-j} \cdot G(X) - \overset{(i)}{F}_1(X^p)\}$$

vor. Es ist aber

$$(39) \qquad [\overset{(i)}{F}_1(X)]^p - \overset{(i)}{F}_1(X^p) \equiv p \cdot \overset{(i)}{F}_1(X) \cdot H(X) \pmod{p^i},$$

wo nach der obigen Bemerkung $H(X)$ modulo p zu $\overset{(i)}{F}_1(X)$ teilerfremd ist. Da nun

$$\bar{O}'(X) = p \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot \overset{(i)}{F}_1(X) \{H(X) + p^{r-1} \cdot G(X) \cdot [\overset{(i)}{F}_1(X)]^{p-j-1}\}$$

ist, so ist leicht ersichtlich, dass man immer ein Polynom $\Theta(X)$ derart finden kann, dass

$$\Theta(X) \cdot \bar{O}'(X) \equiv p \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot \overset{(i)}{F}_1(X) \text{ (modulis } p^i,\ X^{pm}-1)$$

wird, wenn $j < p-1$.[3] Setzen wir nämlich

$$\bar{O}'(X) = p \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot \overset{(i)}{F}_1(X) \cdot H'(X),$$

so genügt es, $\Theta(X)$ modulis p^{i-1}, $\overset{(i)}{F}_1(X^p)$[1] zu finden. In erster Annäherung hat man $\Theta_1(X)$ aus

$$1 \equiv \Theta_1(X) \cdot H'(X) + P_1(X) \cdot \overset{(i)}{F}_1(X^p)$$
$$\equiv \Theta_1(X) \cdot H'(X) + P_1(X) \cdot [\overset{(i)}{F}_1(X)]^p \pmod{p},$$

welche Kongruenz immer möglich ist, da $H(X)$[2] und $\overset{(i)}{F}_1(X)$

[1] oder noch allgemeiner modulis p^{i-1}, $\frac{\overset{(i-1)}{F_1}(X^p)}{\overset{(i-1)}{F_1}(X)}$.

[2] und somit $H'(X)$ für $j < p-1$.

[3] Hinreichende aber keineswegs notwendige Bedingung.

modulo p teilerfremd sind. $\Theta_1(X)$ kann man dann sukzessiv »verbessern», bis man zu

$$1 \equiv \Theta(X) \cdot H'(X) + P(X) \cdot \overset{(i)}{F}_1(X^p) \pmod{p^{i-1}}$$

gelangt. Mit Hilfe von

$$O'(X) = p \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot \overset{(i)}{F}_1(X)$$

können wir

$$O(X) = \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \{[\overset{(i)}{F}_1(X)]^j + p^r \cdot G(X)\}$$

auf die Form

$$\frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \{[\overset{(i)}{F}_1(X)]^j + p^{r'}(\alpha_0 + \alpha_1 X + \cdots + \alpha_{z-1} X^{z-1})\}$$

bringen. Dabei ist also $G'(X) = \alpha_0 + \alpha_1 X + \cdots + \alpha_{z-1} X^{z-1}$ zu $\overset{(i)}{F}_1(X)$ teilerfremd modulo p. Ferner sind nicht alle α_i durch p teilbar. Um nun die Existenz von O'' in $[\Phi(O)]$ nachzuweisen, bilden wir

$$O''(X) = \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \{[\overset{(i)}{F}_1(X)]^j + p^{r'} \cdot G'(X)\}$$

$$\left\{ \frac{\overset{(i)}{F}_1(X^p)}{\overset{(i)}{F}_1(X)} - p^{r'} \cdot G'(X) \cdot [\overset{(i)}{F}_1(X)]^{p-j-1} \right\}$$

$$= p^{r'+1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot G'(X) \{-H(X) - p^{r'-1} \cdot G'(X) [\overset{(i)}{F}_1(X)]^{p-j-1}\}$$

modulis p^i, $X^{pm}-1$. Es gibt dann wie oben ein Polynom $\Theta(X)$, für welches

$$O''(X) \cdot \Theta(X) = O''(X) = p^{r'+1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \text{ (modulis } p^i, X^{pm}-1),$$

und zwar immer für $j < p-1$.[1] Mit Hilfe der Operationen O'', $C^{-1}O''C, \ldots$ können wir nun $\alpha_0, \alpha_1, \ldots, \alpha_{\varkappa-1}$ auf die Werte $0, 1, \ldots, p-1$ beschränken und haben somit die normierte Operation $\bar{O}$ in $[\Phi(O)]$ nachgewiesen. Umgekehrt ist aber offenbar O in $[\Phi(O)]$ enthalten, und also ist, wie behauptet, $[\Phi(O)] = [\Phi(\bar{O})]$.

Wir wenden uns nun dem bisher ausgenommen Falle $j = p-1$ zu und können dabei von

$$O \sim \frac{X^{pm}-1}{\overset{(i)}{F}_1(X)^p} \left\{ \frac{\overset{(i)}{F}_1(X^p)}{\overset{(i)}{F}_1(X)} + p^r \cdot G(X) \right\}$$

ausgehen, da ja

$$[\overset{(i)}{F}_1(X)]^{p-1} \equiv \frac{\overset{(i)}{F}_1(X^p)}{\overset{(i)}{F}_1(X)} \pmod{p} \text{ ist.}$$

Es sei ferner

$$G(X) = K(X) \cdot [\overset{(i)}{F}_1(X)]^j + p \cdot L(X)$$

und zwar derart, dass $K(X)$ nicht modulo p durch $\overset{(i)}{F}_1(X)$ teilbar ist. Dabei kann stets $j < p-2$ vorausgesetzt werden, weil $j = p-1$ auf ein $p^{r'} \cdot G'(X)$ mit $r' > r$ führen würde. *In* $[\Phi(O)]$ *ist immer die Operation*

$$O' \sim p^r \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot [\overset{(i)}{F}(X)]^{j+1}$$

enthalten. Davon überzeugt man sich ganz wie oben, wenn man bemerkt, dass

$$\bar{O}' \sim p^r \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \{K(X) \cdot [\overset{(i)}{F}_1(X)]^{j+1} + p\, L(X) \cdot \overset{(i)}{F}_1(X)\}$$

in $[\Phi(O)]$ vorkommt. Somit kann $K(X)$ durch Zuhilfenahme geeigneter Operationen in $[\Phi(O)]$ auf die Form $K'(X) = \alpha_0 + \alpha_1 X + \cdots \alpha_{\varkappa-1} X^{\varkappa-1}$ gebracht werden. Dabei tritt aber keine

[1] Auch für $j = p-1$, $r' > 1$. Vgl. S. 53.

Vergrösserung von r ein, weil sonst $K(X)$ modulo p durch $\overset{(i)}{F}_1(X)$ teilbar wäre. Ferner betrachten wir

$$\frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)}\left\{\frac{\overset{(i)}{F}_1(X^p)}{\overset{(i)}{F}_1(X)}+p^r\left(K'(X)\,.\,[\overset{(i)}{F}_1(X)]^j+p\,L(X)\right)\right\}\cdot$$

$$\{[F_1(X)]^{p-j-1}-p^r\,.\,K'(X)\}$$

$$\equiv p^{r+1}\cdot\frac{X^{pm}-1}{\overset{(i)}{F}(X^p)}\cdot\{K'(X)\,(H(X)-K'(X)\,.\,[\overset{(i)}{F}_1(X)]^j\,.\,p^{r-1})+$$

$$L(X)\,.\,[\overset{(i)}{F}_1(X)]^{p-j-1}-p^r\,.\,L(X)\,.\,K'(X)\}$$

modulis p^i, $X^{pm}-1$. Wegen $j<p-1$ erkennt man nun leicht, *dass*

$$O''\sim p^{r+1}\cdot\frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)}$$

in $[\Phi(O)]$ *vorkommt*, wenn die Möglichkeit $j=0$, $r=1$ vorläufig beiseite gelassen wird, *und dass somit die Operation*

$$\bar{O}\sim\frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)}\left\{\frac{\overset{(i)}{F}_1(X^p)}{\overset{(i)}{F}_1(X)}+p^r\left(\alpha_0+\alpha_1X+\cdots\alpha_{\varkappa-1}X^{\varkappa-1}\right)[\overset{(i)}{F}_1(X)]^j\right\}$$

auch in $[\Phi(O)]$ *vorkommt.*

Schliesslich ist offenbar $[\Phi(\bar{O})]=[\Phi(O)]$ *und wir haben auch in diesem Falle die gewünschte Normierung.* In demselben Resultate kommen wir auch im Falle $j=0$, $r=1$, *wenn nicht gerade* $K'(X)\equiv H(X)$ (modulis p, $\overset{(i)}{F}_1(X)$). Ist aber $K'(X)=$ $=H(X)+p\,.\,L'(X)+\overset{(i)}{F}_1(X)\,.\,L''(X)$, so wird

$$O\sim\frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)}\{[\overset{(i)}{F}_1(X)]^{p-1}+p\,.\,\overset{(i)}{F}_1(X)\,.\,L''(X)+p^2\,.\,(L(X)+L'(X))\}$$

Man zeigt aber genau wie oben, dass $[\Phi(O)]=[\Phi(O)]$ *für*

$$\bar{O} \sim \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \cdot \{[\overset{(i)}{F}_1(X)]^{p-1} + p^r(\alpha_0 + \alpha_1 X + \cdots \alpha_{\varkappa-1} X^{\varkappa-1})\},$$

$$(\alpha_0, \alpha_1, \ldots, \alpha_{\varkappa-1} = 0, 1, \ldots, p-1),$$

wobei doch r nur die Werte $2, 3, \ldots, i-1$ *annimmt.*

Damit sind alle $\overset{(i)}{H}$ vom Typus $[\Phi(O)]$ erledigt, und wir gehen nun zur Bestimmung aller in $\overset{(i)}{H}_1$ enthaltenen $\overset{(i)}{H}$ und dann auch $\overset{(i-1)}{H}, \ldots, \overset{(1)}{H}$ über. Es sei die H-Gruppe $\overset{(i)}{H}$ in $\overset{(i)}{H}_1$ gegeben. Dann ist es zunächst immer möglich O_1 so zu wählen, dass in $\overset{(i)}{H}$ und $[\Phi(O_1)]$ die Operationen p^i:ter Ordnung bis auf Operationen niedriger Ordnung übereinstimmen. Es ist hinreichend, dass

$$[\Phi(O_1 p^{i-1})] = [\overset{(i)}{H}]^{p^{i-1}},$$

wenn $[\overset{(i)}{H}]^{p^{i-1}}$ die $\overset{(1)}{H}$ bezeichnet, welche aus $\overset{(i)}{H}$ hervorgeht, wenn jede Operation zur p^{i-1}:ten Potenz erhöht wird. Ebenso gibt es eine zweite Operation O_2 von der Ordnung p^{i-1}, welche eine $\overset{(i-1)}{H} = [\Phi(O_2)]$ liefert und zwar derart, dass in $\{[\Phi(O_1)], [\Phi(O_2)]\}$ und unsrer gegebenen $\overset{(i)}{H}$ die Operationen p^i:ter und p^{i-1}:ter Ordnung bis auf Operationen niedriger Ordnung übereinstimmen. Dabei kann O_2 auch $= 1$ sein. So geht es fort, und wir haben allgemein: *Jede* $\overset{(i)}{H}$ *ist in der Form* $\{[\Phi(O_1)], [\Phi(O_2)], \ldots\}$ *darstellbar, wo* $[\Phi(O_1)], [\Phi(O_2)] \ldots$ $\overset{(i)}{H}, \overset{(i-1)}{H} \ldots$ *von den oben gefundenen Typen sind.* Ferner gilt, wie durch Induktion leicht bestätigt wird:

Wenn alle Operationen p^i*:ter Ordnung einer in* $\overset{(i)}{H}_1$ *enthaltenen* $\overset{(i)}{H}$ *nicht bis auf Operationen niedriger Ordnung mit den Op.* p^i*:ter Ordnung der in* $\overset{(i)}{H}_1$ *enthaltenen* $[\Phi(O)]$ für

$$O \sim \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} [\overset{(i)}{F}_1(X) + p^r(\alpha_0 + \alpha_1 X + \cdots \alpha_{\varkappa-1} X^{\varkappa-1})]$$

übereinstimmen, so ist $\overset{(i)}{H} = \overset{(i)}{H}_1 = [\Phi(O)]$ *für*

$$O \sim \frac{X^{pm} - 1}{\overset{(i)}{F}_1(X^p)}.$$

Nach diesen Vorbereitungen finden wir nun für $i > 1$ die gesuchten $\overset{(i)}{H}$ folgendermassen.

1. $[\Phi(O)]$ für

$$O \sim \frac{X^{pm} - 1}{\overset{(i)}{F}_1(X^p)}$$

Ordnung: p^{ip^z}. *Anzahl:* 1.

2. $[\Phi(O)]$ für

$$O \sim \frac{X^{pm} - 1}{\overset{(i)}{F}_1(X^p)} . [\overset{(i)}{F}_1(X)]^j, \; j = 1, 2, \ldots, p-1.$$

Ordnung: $p^{z(i(p-1)-j+1)}$. *Anzahl:* $p-1$.

Die einzigen möglichen Erweiterungen der Gruppen 2 sind

3. $\{[\Phi(O_1)], [\Phi(O_2)]\}$ für

$$O_1 \sim \frac{X^{pm} - 1}{\overset{(i)}{F}_1(X^p)} . [\overset{(i)}{F}_1(X)]^j, \; j = 1, 2, \ldots, p-1,$$

$$O_2 \sim p^r . \frac{X^{pm} - 1}{\overset{(i)}{F}(X^p)}, \; r = 1, 2, \ldots, i-1.$$

Ordnung: $p^{z(ip-j-r+1)}$. *Anzahl:* $(p-1)(i-1)$.

4. $[\Phi(O)]$ für

$$O \sim \frac{X^{pm} - 1}{\overset{(i)}{F}_1(X^p)} \{[\overset{(i)}{F}_1(X)]^j + p^r(\alpha_0 + \alpha_1 X + \cdots + \alpha_{z-1} X^{z-1})\},$$

$$j = 1, 2, \ldots, p-1,$$

$$r = 1, 2, \ldots, i-1,$$

$$\alpha_0, \alpha_1, \ldots, \alpha_{n-1} = 0, 1, \ldots, p-1.$$

Doch dürfen nicht alle α gleichzeitig verschwinden. Ausserdem ist der Fall $j = p-1$, $r = 1$ besonders zu behandeln.

Ordnung: $p^{\varkappa(ip-j-r)}$. *Anzahl:* $(p^{\varkappa}-1)[(p-1)(i-1)-1]$.

Suchen wir die Gruppen 4 zu erweitern durch eine $[\Phi(O_2)]$, so ergiebt sich nichts Neues, da O_2

$$p^{r} \cdot \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)} \text{ oder } p^{r-1} \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)}, p^{r-2} \cdot \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)} \cdots$$

entsprechen muss. Dann wird aber $\{[\Phi(O)], [\Phi(O_2)]\}$ mit einer der Gruppen 3 identisch. Neue Gruppen haben wir dagegen in

5. $[\Phi(O)]$ für

$$O \sim \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)} \left[\frac{\overset{(i)}{F_1}(X^p)}{\overset{(i)}{F_1}(X)} + p^{r}(\alpha_0 + \alpha_1 X + \cdots + \alpha_{\varkappa-1} X^{\varkappa-1})[\overset{(i)}{F_1}(X)]^{j} \right],$$

$$j = 0, 1, \ldots, p-2,$$

$$r = 1, 2, \ldots, i-1,$$

$$\alpha_0, \alpha_1, \ldots, \alpha_{\varkappa-1} = 0, 1, \ldots, p-1.$$

α_i nicht gleichzeitig 0. Der Ausnahmefall

$$j = 0, r = 1, \alpha_0 + \alpha_1 X + \cdots + \alpha_{\varkappa-1} X^{\varkappa-1} \equiv H(X) \text{ (modulis } p, \overset{(i)}{F_1}(X))$$

ist schon unter 4 oder 2 mitgerechnet.

Ordnung: $p^{\varkappa(ip-pr-j+r-1)}$. *Anzahl:* $(p^{\varkappa}-1)(p-1)(i-1)-1$.

Bei Erweiterung der Gruppen 5 durch irgend eine $[\Phi(O_2)]$ ergibt sich immer eine $\overset{(i)}{H}$, welche $[\Phi(O_1)]$ für

$$O_1 \sim \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)} \cdot \frac{\overset{(i)}{F_1}(X^p)}{\overset{(i)}{F_1}(X)}$$

enthält. Dies findet man leicht bei Durchmusterung der verschiedenen Typen $[\Phi(O_2)]$, wenn man noch bemerkt, dass jede Gruppe 5 die Operationen O_1, O_2, O_3 enthält, welche

$$p^{r+1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)}, \quad p \cdot \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)} \cdot \frac{\overset{(i)}{F_1}(X^p)}{\overset{(i)}{F_1}(X)}, \quad p^r \cdot \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)} \cdot [\overset{(i)}{F_1}(X)]^{j+1}$$

entsprechen. Wir müssen nun also schliesslich diejenigen $\overset{(i)}{H}$ aufsuchen, welche die Gruppe $[\Phi(O)]$ für

$$O \sim \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)} \cdot \frac{\overset{(i)}{F_1}(X^p)}{\overset{(i)}{F_1}(X)}$$

enthalten, und haben als

6. diese $[\Phi(O)]$ selbst.

Ordnung: p^{xi}. *Anzahl:* 1.

Die Gruppe 6 durch Gruppen vom Typus 1 erweitert gibt

7. $\{[\Phi(O_1)], [\Phi(O_2)]\}$ für

$$O_1 \sim \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)} \cdot \frac{\overset{(i)}{F_1}(X^p)}{\overset{(i)}{F_1}(X)},$$

$$O_2 \sim p^r \cdot \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)}, \quad r = 2, 3, \ldots, i-1.$$

Ordnung: $p^{x(ip-rp+r)}$. *Anzahl:* $i-2$.

Der Fall $r = 1$ ist schon unter 3 mitgenommen, weil gleichzeitig mit O_1 und O_2 auch

$$O_3 \sim \frac{X^{pm}-1}{\overset{(i)}{F_1}(X^p)} \cdot [\overset{(i)}{F_1}(X)]^{p-1}$$

in $\overset{(i)}{H}$ vorkommt. Hieraus folgt dann ferner,[1] dass wir bei Erweiterung von der Gruppe 6 durch $[\Phi(O_2)]$ vom Typus 2 nur die Werte $1, 2, \ldots, p-2$ von j zu berücksichtigen brauchen. Diese liefern aber verschiedene Gruppen, und wir haben

8. $\{[\Phi(O_1)], [\Phi(O_2)]\}$ für

$$O_1 \sim \frac{X^{p^m}-1}{\overset{(i)}{F_1}(X^p)} \cdot \frac{\overset{(i)}{F_1}(X^p)}{\overset{(i)}{F_1}(X)},$$

$$O_2 \sim p^r \frac{X^{p^m}-1}{\overset{(i)}{F_1}(X^p)} \cdot [\overset{(i)}{F_1}(X)]^j,$$

$$j = 1, 2, \ldots, p-2,$$

$$r = 1, 2, \ldots, i-1.$$

Ordnung: $p^{\varkappa(ip-p^r-j+r)}$. *Anzahl:* $(p-2)(i-1)$.

Eine Erweiterung von 6 durch $[\Phi(O)]$ vom Typus 3, 4 oder 5 liefert nichts Neues. Dies ist für die Fälle 3 und 5 einleuchtend. Um die Richtigkeit unserer Behauptung auch für den Fall 4 nachzuweisen, bemerken wir, dass gleichzeitig mit

$$O_1 \sim \frac{X^{p^m}-1}{\overset{(i)}{F_1}(X^p)} \cdot \frac{\overset{(i)}{F_1}(X^p)}{\overset{(i)}{F_1}(X)}$$

und

$$O_2 \sim p^r \cdot \frac{X^{p^m}-1}{\overset{(i)}{F_1}(X^p)} \{[\overset{(i)}{F_1}(X)]^j + p^s(\alpha_0 + \alpha_1 X + \cdots \alpha_{z-1} X^{z-1})\}$$

auch

$$O_3 \sim p^{r+1} \cdot \frac{X^{p^m}-1}{\overset{(i)}{F}(X^p)} \cdot \overset{(i)}{F_1}(X)$$

---

[1] $[\overset{(i)}{F_1}(X)]^{p-1} - \dfrac{\overset{(i)}{F_1}(X^p)}{\overset{(i)}{F_1}(X)} \equiv p \cdot H(X) \pmod{p^i, \overset{(i)}{F_1}(X^p)}$; $\theta(X) \cdot H(X) \equiv 1 \pmod{\text{modulis}}$ ist immer lösbar, d. h. gleichzeitig mit O_1, und O_3 kommt O_2 in $\overset{(i)}{H}$ vor.

und somit

$$O_4 \sim p^{r+2} \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)}$$

in $\{[\Phi(O_1)], [\Phi(O_2)]\}$ vorkommt. Also kann zunächst s auf den Wert 1 beschränkt werden. Dann aber ist $j \leq p-2$ zu setzen, und in

$$O_5 \sim p^r \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \{[\overset{(i)}{F}_1(X)]^{p-1} + p(\alpha_0 + \alpha_1 X + \cdots \alpha_{z-1} X^{z-1})[\overset{(i)}{F}_1(X)]^{p-1-j}\}$$

ist $p-1-j \neq 0$. Es kommt nun

$$O_5\, O_1^{-p^r} \sim p^r \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} \left\{ [\overset{(i)}{F}_1(X)]^{p-1} - \frac{\overset{(i)}{F}_1(X^p)}{\overset{(i)}{F}_1(X)} + p(\alpha_0 + \alpha_1 X + \cdots \alpha_{z-1} X^{z-1})[\overset{(i)}{F}_1(X)]^{p-1-j} \right\}$$

in $\{[\Phi(O_1)], [\Phi(O_2)]\}$ vor. Da aber

$$O_5 \cdot O_1^{-p^r} \sim p^{r+1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)} [H(X) + (\alpha_0 + \alpha_1 X + \cdots \alpha_{z-1} X^{z-1})[\overset{(i)}{F}_1(X)]^{p-j-1}]$$

und $p-j-1 \neq 0$ ist, so kommt offenbar

$$O_6 \sim p^{r+1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F}(X^p)}$$

in unserer Gruppe vor, und diese ist somit vom Typus 8.

Mit 1—8 haben wir alle $\overset{(i)}{H}$ in $\overset{(i)}{H}_1$ erschöpft. *Ihre Anzahl wird für* $i \geq 2$

$$N_i = 2p^z(p-1)i - 2p^{z+1} + p^z + p,$$

während $N_1 = p$. Wenn man noch die Einheit mitrechnet, wird also *die Anzahl aller in* $\overset{(i)}{H}_1$ *enthaltenen H-Gruppen*

$$N_i = 1 + p + \sum_2^i N_i = 1 + p + \\ + p^x(p-1)(i-1)\,i - p(p^{x-1}-1)(i-1).$$

Bildet man nun die Zahl N_i *für alle irreduziblen Faktoren modulo* p *von* $X^m - 1$, *so ist*

$$N_i = N_i^{(1)} \cdot N_i^{(2)} \dots N_i^{(s)}$$

die Anzahl aller H-Gruppen in $[\Sigma_0, \Sigma_1, \dots, \Sigma_{pm-1}]$.

So haben wir für $p = 2, m = 3, i = 2$,

$$X^3 - 1 = \overset{(2)}{F}_1 \cdot \overset{(2)}{F}_2 = (X-1)(X^2 + X + 1),$$

$x_1 = 1$, $x_2 = 2$, $N_2^{(1)} = 7$, $N_2^{(2)} = 9$ als Anzahl der H-Gruppen in $[\Sigma_0, \Sigma_1, \dots, \Sigma_5] : 7 \cdot 9 = 63$. Für $p = 2$, $m = x = 1$, wird $N_i = 3 + 2i(i-1)$. Die $\overset{(i)}{H}$-Gruppen sind die folgenden:

1. $[\Phi(O)]$ für
$$O \sim 1;$$
2. $[\Phi(O)]$ für
$$O \sim x - 1;$$
3. $\{[\Phi(O_1)], [\Phi(O_2)]\}$ für
$$O_1 \sim x - 1$$
$$O_2 \sim 2^r,\ r = 1, 2, \dots, i-1;$$
4. $[\Phi(O)]$ für
$$O \sim x - 1 + 2^r,\ r = 2, 3, \dots, i-1;$$
5. $[\Phi(O)]$ für
$$O \sim x + 1 + 2^r,\ r = 2, 3, \dots, i-1;$$
6. $[\Phi(O)]$ für
$$O \sim x + 1;$$

7. $\{[\Phi(O_1)], [\Phi(O_2)]\}$ für

$$O_1 \sim x + 1$$

$$O_2 \sim 2^r,\ r = 2, 3, \ldots, i-1.$$

Die zu einer H-Gruppe gehörigen Charaktere können wegen ihrer reziproken Beziehung zu den H-Gruppen auf Gruppen von Charakteren verteilt werden, welche den $\overset{(i)}{H}_1$, $\overset{(i)}{H}_2, \ldots, \overset{(i)}{H}_s$ analog sind. Ist $\bar{\Phi}_x$ ein Polynom, welches in der angegebenen Weise[1] einem Charakter irgend welcher H-Gruppe entspricht, so ist also

$$\bar{\Phi}_x = \sum_{j=1}^{j=s} G_j(X) \frac{X^{p^m}-1}{\overset{(i)}{F}_j(X^p)}.$$

$G_j(X)$ irgend eines der modulis p^i, $\overset{(i)}{F}_j(X^p)$ verschiedenen Polynome. Ausserdem entsprechen die Φ_x von der Form $G_j(X) \cdot \frac{X^{p^m}-1}{\overset{(i)}{F}_j(X^p)}$, welche zu unserer H-Gruppe gehören, einer in $\overset{(i)}{H}_j$ enthaltenen H-Gruppe. Da ferner jedes $\Phi_x \sim G(X) \cdot \frac{X^{p^m}-1}{\overset{(i)}{F}_j(X^p)}$ zu allen $\overset{(i)}{H}_1, \overset{(i)}{H}_2, \ldots, \overset{(i)}{H}_s$ mit Ausnahme von $\overset{(i)}{H}_j$ gehört, so ist es offenbar hinreichend für die Auffindung aller zu

$$H = H_1 . H_2 \ldots H_s \,(H_j \text{ in } \overset{(i)}{H}_j)$$

gehörigen Polynome, diejenigen von der Form $G(X) \cdot \frac{X^{p^m}-1}{\overset{(i)}{F}_j(X^p)}$ aufzustellen, welche zu H_j gehören. Diese findet man aber leicht. *Nehmen wir zunächst an H_j sei eine $\overset{(i)}{H}$*, so haben wir für die Typen 1—8 folgende $\bar{\Phi}_x$ von der Form $G(X) \cdot \frac{X^{p^m}-1}{\overset{(i)}{F}_j(X^p)}$.

[1] S. 7.

1. $\Phi_x = 0;$

2. $$\bar{\Phi}_x = G_1(X) \cdot \frac{X^{pm}-1}{\overset{(i)}{F_j}(X^p)} \cdot \frac{\overset{(i)}{F_j}(X^p)}{\overset{(i)}{F_j}(X)} + \\ + G_2(X) \cdot p^{i-1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F_j}(X^p)} [\overset{(i)}{F_j}(X)]^{p-j};$$

3. $$\overline{\Phi}_x = G_1(X) \cdot p^{i-r} \cdot \frac{X^{pm}-1}{\overset{(i)}{F_j}(X^p)} \cdot \frac{\overset{(i)}{F_j}(X^p)}{\overset{(i)}{F_j}(X)} + \\ + G_2(X) \cdot p^{i-1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F_j}(X^p)} \cdot [\overset{(i)}{F_j}(X)]^{p-j};$$

4. $$\bar{\Phi}_x = G(X) \cdot p^{i-r-1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F_j}(X^p)} \left\{ \frac{\overset{(i)}{F_j}(X^p)}{\overset{(i)}{F_j}(X)} - p^r(\alpha_0 + \right. \\ \left. + \alpha_1 X + \cdots \alpha_{\varkappa_j - 1} X^{\varkappa_j - 1}) [\overset{(i)}{F_j}(X)]^{p-j-1} \right\};$$

5. $$\overline{\Phi}_x = G(X) \cdot p^{i-r-1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F_j}(X^p)} \{ [\overset{(i)}{F}(X)]^{p-j-1} - \\ - p^r(\alpha_0 + \alpha_1 X + \cdots + \alpha_{\varkappa_j - 1} X^{\varkappa_j - 1}) \};$$

6. $$\overline{\Phi}_x = G(X) \cdot \frac{X^{pm}-1}{\overset{(i)}{F_j}(X^p)} \cdot \overset{(i)}{F_j}(X);$$

7. $$\bar{\Phi}_x = G(X) \cdot p^{i-r} \cdot \frac{X^{pm}-1}{\overset{(i)}{F_j}(X^p)} \cdot \overset{(i)}{F_j}(X);$$

8. $$\overline{\Phi}_x = G(X) \cdot p^{i-r-1} \cdot \frac{X^{pm}-1}{\overset{(i)}{F_j}(X^p)} \cdot [\overset{(i)}{F_j}(X)]^{p-j}.$$

Ist H_j eine $\overset{(i-t)}{H}$, so haben wir nur $i-t$ statt i in den schon gefundenen Φ_x zu schreiben. In den Fällen 1, 6, 7, 8

kommen noch $G(X) \cdot p^{i-t} \cdot \dfrac{X_{p^m}-1}{\overset{(i)}{F_j}(X^p)}$ zu den bereits gefundenen hinzu.

Die Gruppen von Typus 2 (S. 54) können mit denjenigen vom Typus 3 zum Typus $\{[\Phi(O_1)], [\Phi(O_1)]\}$ für

$$O_1 \sim \frac{X^{p^m}-1}{\overset{(i)}{F_1}(X^p)} [\overset{(i)}{F_1}(X)]^j, \quad j = 1, 2, \ldots, p-1,$$

$$O_2 \sim p^r \cdot \frac{X^{p^m}-1}{\overset{(i)}{F_1}(X^p)}, \qquad r = 1, 2, \ldots, i,$$

zusammengefasst werden. Ebenso die Typen 6, 7, 8 zum $\{[\Phi(O_1)], [\Phi(O_2)]\}$ für

$$O_1 \sim \frac{X^{p^m}-1}{\overset{(i)}{F_1}(X^p)} \cdot \frac{\overset{(i)}{F_1}(X^p)}{\overset{(i)}{F_1}(X)},$$

$$O_2 \sim p^r \cdot \frac{X^{p^m}-1}{\overset{(i)}{F_1}(X^p)} [\overset{(i)}{F_1}(X)]^j,$$

$$j = 1, 2, \ldots, p-1,$$
$$r = 1, 2, \ldots, i-1.$$

Eine Gruppe der ersteren Art bezeichnen ich $\overset{(i-t)}{H_{\mathrm{II}}}(j; r)$, eine der zweiten $\overset{(i-t)}{H_{\mathrm{V}}}(j; r)$, wenn $p^t O(X)$ statt $O(X)$ steht.

Ferner setze ich $\overset{(i-t)}{H_{\mathrm{III}}}(j; r; \alpha_0, \alpha_1, \ldots, \alpha_{\varkappa-1}) = [\Phi(O)]$ für

$$O \sim p^t \cdot \frac{X^{p^m}-1}{\overset{(i)}{F_1}(X^p)} \{[\overset{(i)}{F_1}(X)]^j + p^r(\alpha_0 + \alpha_1 X + \cdots + \alpha_{\varkappa-1} X^{\varkappa-1})\}$$

und $\overset{(i-t)}{H_{\mathrm{IV}}}(j; r; \alpha_0, \alpha_1, \ldots, \alpha_{\varkappa-1}) = [\Phi(O)]$ für

$$O \sim p^t \cdot \frac{X^{p^m}-1}{\overset{(i)}{F_1}(X^p)} \left\{ \frac{\overset{(i)}{F_1}(X^p)}{\overset{(i)}{F_1}(X)} + p^r(\alpha_0 + \alpha_1 X + \cdots + \alpha_{\varkappa-1} X^{\varkappa-1}) [\overset{(i)}{F_1}(X)]^j \right\}.$$

Wenn wir $r=0$ in den $\overset{(i-t)}{H_{\mathrm{V}}}$ zulassen, so wird $\overset{(i-t)}{H_{\mathrm{V}}}(j; 0) = \overset{(i-t)}{H_{\mathrm{II}}}(j; 1)$.

Es ist

$$\overset{(i-t)}{H}_{\mathrm{III}}(p-1;1;\alpha_0,\alpha_1,\ldots,\alpha_{\varkappa-1})=\overset{(i-t)}{H}_{\mathrm{IV}}(0;1;\alpha_0+\bar{\alpha}_0,\alpha_1+\bar{\alpha}_1,\ldots,\alpha_{\varkappa-1}+\alpha_{\varkappa-1}),$$

falls

$$\frac{1}{p}\left\{[\overset{(i)}{F}_1(X)]^{p-1}-\frac{\overset{(i)}{F}_1(X^p)}{\overset{(i)}{F}_1(X)}\right\}\quad \alpha_0+\alpha_1 X+\cdots+\bar{\alpha}_{\varkappa-1}X^{\varkappa-1}$$

(modulis $p, \overset{(i)}{F}_1(X)$).

Dabei muss doch der Fall $\alpha_0\equiv-\bar{\alpha}_0, \alpha_1\equiv-\bar{\alpha}_1, \ldots, \alpha_{\varkappa-1}\equiv-\bar{\alpha}_{\varkappa-1}$ ausgenommen werden, weil dann die Gruppe $\overset{(i-t)}{H}_{\mathrm{III}}$ nicht immer mit $\overset{(i-t)}{H}_{\mathrm{IV}}(0;1;0,0,\ldots,0)=\overset{(i-t)}{H}_{\mathrm{V}}(p-1,i-t-1)$ identisch ist. Schliesslich sei $\overset{(i-t)}{H}_{\mathrm{I}}=[\Phi(O)]$ für

$$O\sim p^t\cdot\frac{X^{pm}-1}{\overset{(i)}{F}_j X^p)}.$$

Dann können wir die H-Gruppen in $\overset{(i)}{H}_1$ in folgender Weise zusammenstellen:

$\overset{(i-t)}{H}_{\mathrm{I}}$	$\overset{(t)}{H}_{\mathrm{I}}$
$\overset{(i-t)}{H}_{\mathrm{II}}(j;r)$	$\overset{(r+t)}{H}_{\mathrm{V}}(p-j;r-1)$
$\overset{(i-t)}{H}_{\mathrm{II}}(j;1)$	$\overset{(r+t)}{H}_{\mathrm{II}}(p-j;1)$
$\overset{(i-t)}{H}_{\mathrm{III}}(j;r;\alpha_0,\alpha_1,\ldots,\alpha_{\varkappa-1})$	$\overset{(r+t+1)}{H}_{\mathrm{IV}}(p-j-1;r;p-\alpha_0,p-\alpha_1,\ldots,p-\alpha_{\varkappa-1})$
$\overset{(i-t)}{H}_{\mathrm{IV}}(j;r;\alpha_0,\alpha_1,\ldots,\alpha_{\varkappa-1})$	$\overset{(r+t+1)}{H}_{\mathrm{III}}(p-j-1;r;p-\alpha_0,p-\alpha_1,\ldots,p-\alpha_{\varkappa-1})$
$\overset{(i-t)}{H}_{\mathrm{IV}}(0;1;\alpha_0,\alpha_1,\ldots,\alpha_{\varkappa-1})$	$\overset{(2+t)}{H}_{\mathrm{IV}}(0;1;\bar{\alpha}_0-\alpha_0,\bar{\alpha}_1-\alpha_1,\ldots,\bar{\alpha}_{\varkappa-1}-\alpha_{\varkappa-1})$
$\overset{(i-t)}{H}_{\mathrm{V}}(j;r)$	$\overset{(r+t+1)}{H}_{\mathrm{II}}(p-j;r+1)$.

Die in derselben Zeile stehenden H-Gruppen entsprechen einander derart, dass die $O(X)$ der einen die zur zweiten gehörigen Polynome von der Form $G(X)\cdot\frac{X^{pm}-1}{\overset{(i)}{F}_1(X^p)}$ sind. *Ist*

nun $H_1 . H_2 \ldots H_s$ *eine beliebige H-Gruppe* (H_1 in $\overset{(i)}{H}_1, \ldots$) *und sind* $H'_1, H'_2, \ldots$ *die* $H_1, H_2, \ldots$ *nach dem obigen Schema entsprechenden Gruppen, so hat man in den* $O(X)$ *der Gruppe* $H'_1 . H'_2 \ldots H'_s$ *alle zu* $H_1 . H_2 \ldots$ *gehörigen Polynome.*

IV. Die Ordnung der Σ_i eine beliebige Zahl.

Da jede ABEL'sche Gruppe als Produkt von Gruppen, deren Operationen von Primzahlpotenzordnung sind, darstellbar ist, zeigen wir leicht, dass dieser Fall sofort erledigt wird, wenn unsere Aufgabe in den Fällen I, II, III gelöst ist. Es müssen ja diese Gruppen mit Operationen von Primzahlpotenzordnung selbst H-Gruppen sein. *Insbesondere können wir also für beliebige Ordnungen der* Σ_i *alle in* $\{\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}\}$ *enthaltenen H-Gruppen bestimmen, wenn* m *eine Primzahl oder das Produkt* pq *zweier verschiedenen Primzahlen ist.*

V. Über $H(\Sigma, \sigma)$-Gruppen.

Wir wollen nun den Kreis unsrer Betrachtungen dadurch erweitern, dass wir nebst den Operationen $\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}$ von der Primzahlordnung p die m neuen Operationen $\sigma_0, \sigma_1, \ldots, \sigma_{m-1}$ einführen. Es ist dabei

$$\sigma_i = (1^{(i)}\, \lambda^{(i)}\, \lambda^{(i)2} \ldots \lambda^{(i)p-2})$$

wenn, wie oben,

$$\Sigma_i = (1^{(i)}\, 2^{(i)} \ldots p^{(i)})$$

gesetzt wird, und die Potenzen der primitiven Wurzel λ modulo p genommen werden. Die σ_i sind vertauschbar, und es gilt

$$\sigma_i^{-1}\, \Sigma_i\, \sigma_i = \Sigma_i^{\lambda},$$

$$\sigma_i^{-1}\, \Sigma_j\, \sigma_i = \Sigma_j . (j \neq i).$$

$\{\Sigma_i, \sigma_i\}$ ist die vollständige metazyklische Gruppe in den p Elementen $1^{(i)}, 2^{(i)}, \ldots, p^{(i)}$. Ferner ist $C^{-1}\, \sigma_i\, C = \sigma_{i+1}$.

Dies vorausgeschickt, suchen wir alle Untergruppen von $G_{\substack{m \\ p(p-1)}}{}_{m} = \{\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}, \sigma_0, \sigma_1, \ldots, \sigma_{m-1}\}$ zu finden, welche

1. *bei zyklischer Verschiebung sowohl der* Σ- *als der* σ-*Indices ungeändert bleiben,* und
2. *die Elemente* $1^{(i)}, 2^{(i)}, \ldots, p^{(i)}$, $(i = 0, 1, \ldots, m-1)$, *transitiv vertauschen.* Solche Gruppen nenne ich auch H-Gruppen und bezeichne sie mit $H(\Sigma, \sigma)$. Darunter sind insbesondere die bisher betrachteten $H(\Sigma)$.

Es ist zunächst einleuchtend, dass *jede* $H(\Sigma, \sigma)$ *eine von der Einheit verschiedene* $H(\Sigma)$ *enthält.* Der Inbegriff aller Operationen in $H(\Sigma, \sigma)$, welche keine σ enthalten, ist in der Tat eine $H(\Sigma)$, und diese Gruppe muss, der zweiten obenstehenden Bedingung zufolge, $\neq 1$ sein. Ferner folgt aus der Definition der σ_i, dass diese $H(\Sigma)$ eine *invariante Untergruppe von* $H(\Sigma, \sigma)$ *sein muss.* Wir unterscheiden zwei Möglichkeiten:

1. *Die grösste in* $H(\Sigma, \sigma)$ *enthaltene* $H(\Sigma)$ *ist mit* $\{\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}\}$ *identisch,* und
2. *Diese* $H(\Sigma)$ *ist* $< \{\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}\}$.

Der erste Fall lässt sich sofort auf die Bestimmung von $H(\Sigma)$-Gruppen zurückführen. Es ist ja $H(\Sigma, \sigma) = \{\Sigma_0, \Sigma_1, \ldots, \Sigma_{m-1}\}$. $H(\sigma)$, wo $H(\sigma)$ eine Untergruppe von $\{\sigma_0, \sigma_1, \ldots, \sigma_{m-1}\}$ ist, welche die Bedingung $C^{-1} H(\sigma) C = H(\sigma)$ erfüllt. Wir können also zum *zweiten Falle* übergehen. Schon oben haben wir bemerkt, dass jede $H(\Sigma)$ $p-1$ *für die Gruppe charakteristische Operationen* $\bar{O}^i \sim i \dfrac{X^m - 1}{F}$ $(i = 1, 2, \ldots, p-1)$ enthält. Diese müssen somit bei Transformation mit den Operationen unserer $H(\Sigma, \sigma)$ in einander übergehen. Es sei $O = \Sigma_0^{\alpha_0} \Sigma_1^{\alpha_1} \ldots \Sigma_{m-\varkappa}^{\alpha_{m-\varkappa}}$, d. h.

$$\bar{O} \sim \alpha_0 + \alpha_1 X + \cdots + \alpha_{m-\varkappa} X^{m-\varkappa} \quad (\alpha_0, \alpha_{m-\varkappa} \not\equiv 0 \pmod{p}),$$

und $\Pi \sigma_i^{x_i}$ der aus σ_i bestehende Teil einer beliebigen Operation $\Pi \Sigma_i^{y_i} . \Pi \sigma_i^{x_i}$ der $H(\Sigma, \sigma)$. x_0 nehmen wir $\neq 0$ an. Weil O bei Transformation mit $\Pi \sigma_i^{x_i}$ in etwa $\bar{O}^{\prime\prime}$ übergeht, schliessen wir sofort, dass

$$x_{m-\varkappa} = x_0 \neq 0$$

sein muss. Allgemein ist $x_i = x_0$, wenn α_i in O von 0 ver-

schieden ist Nun sind zwei Möglichkeiten aus einander zu halten. *Erstens* kann es ein $\alpha_i \neq 0$ in O geben, dessen Index i zu m relativ prim ist, *zweitens* kann O nur solche Σ_i enthalten, deren Indices nicht zu m relativ prim sind.

Im ersten Fall sei i zu m teilerfremd. Dann ergibt sich sofort, dass

$$\Pi \sigma_i^{x_i} = (\sigma_0 \sigma_1 \ldots \sigma_{m-1})^{x_0}$$

sein muss. Denn es ist $x_0 = x_i$. In Operationen der $H(\Sigma, \sigma)$ kommt aber auch $C^i \Pi \sigma_i^{x_i} C^{-i} = \Pi \sigma_i^{x'_i}$ vor. Hierin ist $x'_0 = x_i = x_0 \neq 0$, und dann muss wie oben auch $x'_i = x'_0 = x_0$ sein. Da nun $x'_i = x_{2i}$, so folgt

$$x_0 = x_i = x_{2i}.$$

Dasselbe Verfahren führt durch Wiederholung zu

$$x_0 = x_i = x_{2i} = \ldots = x_{(m-1)i},$$

wo die Indices modulo m zu nehmen sind. Da i zu m teilerfremd ist, folgt unsere Behauptung. Es ergibt sich ferner, *dass alle* $H(\Sigma, \sigma)$ *von der Form* $\left\{H(\Sigma), (\sigma_0 \sigma_1, \ldots \sigma_{m-1})^{\frac{p-1}{d}}\right\}$ *sind, oder mit einer solchen Gruppe isomorph.* Suchen wir unter allen $\Pi \Sigma_i^{a_i} (\sigma_0 \sigma_1 \ldots \sigma_{m-1})^{\beta}$ in $H(\Sigma, \sigma)$ eine aus, für welche der gemeinschaftliche Teiler von β und $p-1$ so klein als möglich ausfällt, so sind, wenn $\frac{p-1}{d}$ dieser Teiler ist, alle β von der Form $k \cdot \frac{p-1}{d}$. Nehmen wir einen Augenblick an, es gäbe zwei Operationen

$$O = \Pi \Sigma_i^{a_i} (\sigma_0 \sigma_1 \ldots \sigma_{m-1})^{k \cdot \frac{p-1}{d}}$$

$$O' = \Pi \Sigma_i^{a'_i} (\sigma_0 \sigma_1 \ldots \sigma_{m-1})^{k \cdot \frac{p-1}{d}}$$

in $H(\Sigma, \sigma)$, in welchen $\Pi \Sigma_i^{a_i}$ und $\Pi \Sigma_i^{a'_i}$ nicht bis auf Operationen in $H(\Sigma)$ übereinstimmen. Dann muss $OO'^{-1} = \Pi \Sigma_i^{a_i} \Pi \Sigma_i^{-a'_i}$ in $H(\Sigma)$ vorkommen, was der Voraussetzung widerspricht.

Somit ist unsere $H(\Sigma, \sigma)$ *von der Form* $\left\{H(\Sigma), \Pi \Sigma_i^{a_i}(\sigma_0 \sigma_1 \dots \sigma_{m-1})^{\frac{p-1}{d}}\right\}$, und es erübrigt nur die Bestimmung (bis auf Operationen in $H(\Sigma)$) von $\Pi \Sigma_i^{a_i}$. Ist aber

$$\bar{O} \sim \frac{X^m - 1}{(X-1)^i \cdot F_1}, \quad (F_1 \text{ nicht durch } X-1 \text{ teilbar mod. } p),$$

so kann man offenbar

$$\Pi \Sigma_i^{a_i} = \bar{O}' \sim r \cdot \frac{X^m - 1}{(X-1)^{i+1} F_1}, \quad r = 0, 1, \dots, p-1,$$

setzen. i geht von O bis $p^s - 1$, falls m durch p^s teilbar ist. Für $i = p^s$ ist $\bar{O}' = 1$ zu setzen. Wir haben also gefunden, dass *unsere* $H(\Sigma_1 \sigma)$ *in diesem ersten Falle auf die Form* $\left\{[\Phi(O)], O', (\sigma_0 \sigma_1 \dots \sigma_{m-1})^{\frac{p-1}{d}}\right\}$ *gebracht werden können.*[1]

Wir gehen nun zum *zweiten Falle* über, wo alle Indices der in $\bar{O} = \Sigma_0^{a_0} \Sigma_1^{a_1} \dots \Sigma_{m-\varkappa}^{a_{m-\varkappa}}$ auftretenden Σ_i von 1 verschiedene Teiler mit m gemeinsam haben. Es seien m' und m'' zwei solche Teiler. Dann schliessen wir genau wie im vorigen Falle, dass in jeder $\Pi \sigma_i^{x_i}$, welche in $H(\Sigma, \sigma)$ vorkommt,

$$x_0 = x_{0+m'} = x_{0+2m'} = \dots = x_{0+\left(\frac{p-1}{m'}-1\right)m'}$$

$$x_0 = x_{0+m''} = x_{0+2m''} = \dots = x_{0+\left(\frac{p-1}{m''}-1\right)m''}$$

$$x_{0+m'} = x_{0+m'+m''} = x_{0+m'+2m''} = \dots$$

und allgemein $x_0 = x_{k'm'+k''m''}$, wenn, wie wir annehmen wollen, $x_0 \neq 0$ ist. Sind dann m' und m'' teilerfremd, so kommen wir auf den ersten Fall zurück, weil alle Zahlen $1, 2, \dots, m-1$ in der Form $k'm' + k''.m''$ darstellbar sind. Es bleibt also nur die Möglichkeit übrig, dass *die gemeinschaftlicher Teiler* $m', m'', \dots$, *alle Multipeln eines kleinsten von* 1 *verschiedenen Teilers* $\bar{m}$ *sind. Dann muss* $\Pi \sigma_i^{x_i}$ *von der Form*

[1] Durch Transformation mit einer geeigneten $\Pi \Sigma_i^{a_i}$ kann $\bar{O}'$ entfernt werden.

$H\left(\sigma_i \sigma_{i+m} \ldots \sigma_{i+\binom{m}{m-1} m}\right)^{x_i}$ *sein.* $i = 0, 1, \ldots, m-1$. Der Gruppe $H(\Sigma)$ entspricht ein Faktor $F(X^m)$.

Denken wir uns in den Operationen der Gruppe $H(\Sigma, \sigma)$ die Σ_i weggewischt, so bilden die zurückbleibenden $H \sigma_i^{x_i}$ eine $H(\sigma)$, welche offenbar mit $H(\Sigma, \sigma)$ isomorph ist und zwar derart, dass die Einheit der Gruppe $H(\sigma)$ der Gruppe $H(\Sigma)$ in $H(\Sigma, \sigma)$ entspricht. Zwei Operationen in $H(\Sigma, \sigma)$, welche in den σ übereinstimmen, können sich nur durch eine Operation in $H(\Sigma)$ unterscheiden, da ja $O O'^{-1}$ keine σ_i enthält. Um nun die Struktur der mit den σ vereinten Σ näher zu untersuchen, führen wir eine neue Indizierung ein, indem wir

$$\Sigma_{i,j} = \Sigma_{i+j.\,m}, \begin{pmatrix} i = 0, 1, \ldots, m-1 \\ j = 0, 1, \ldots, \frac{m}{m} - 1 \end{pmatrix}$$

setzen.[1] Es ist dann

$$H(\Sigma) = H_0(\Sigma) . H_1(\Sigma) \ldots H_{m-1}(\Sigma),$$

wenn $H_0(\Sigma)$ in $\{\Sigma_{0,0}, \Sigma_{0,1}, \ldots, \Sigma_{0,\frac{m}{m}-1}\}$ enthalten ist und die Bedingung $C^{-m} H_0(\Sigma) C^m = H_0(\Sigma)$ erfüllt, und ausserdem $H_i(\Sigma) = C^{-i} H_0(\Sigma) C^i$ ist. Wir erkennen dann wie oben, das die überhaupt möglichen Formen einer $H \Sigma_{i,j}^{a_{i,j}} H \sigma_{i,j}^{\beta_{i,j}}$ in $H(\Sigma, \sigma)$ sich auf

$$H \bar{O}'^{a_i}_i H \left(\sigma_{i,0} \sigma_{i,1} \ldots \sigma_{i,\frac{m}{m}-1}\right)^{\beta_i}$$

reduzieren, wenn von Operationen in $H(\Sigma)$ abgesehen wird. Es ist dabei für

$$\bar{O}_0 = \frac{X^m - 1}{(X^{\bar{m}} - 1)^i . F_1(X^{\bar{m}})} \quad \begin{matrix} (F_1(X) \text{ nicht durch} \\ X - 1 \text{ teilbar}) \end{matrix}$$

$$\bar{O}'_0 = \frac{X^m - 1}{(X^{\bar{m}} - 1)^{i+1} . F_1(X^{\bar{m}})}$$

zu setzen und ferner

[1] und ebenso $\sigma_{i,j} = \sigma_{i+j.\,m}$.

$$O'_i = C^{-i} \bar{O}'_0 C^i.$$

Für $\frac{m}{m} = p^s . m'$, $i = p^s$ hat man $O'_0 = 1$ zu wählen. Nehmen wir alle $\alpha_i = 0$ an, so ist der Inbegriff aller in $H(\Sigma, \sigma)$ vorkommenden $\Pi \left(\sigma_{i,0}\, \sigma_{i,1} \ldots \sigma_{i,\frac{m}{m}-1}\right)^{\beta_i}$ offenbar eine Untergruppe von $\left\{\sigma_{0,0}\, \sigma_{0,1} \ldots \sigma_{0,\frac{m}{m}-1}, \sigma_{1,0}\, \sigma_{1,1} \ldots \sigma_{1,\frac{m}{m}-1}, \ldots\right\}$, welche bei Transformation mit C ungeändert bleibt, und deren Auffindung mit der Bestimmung aller $H(\sigma)$ in $\{\sigma_0, \sigma_1, \ldots, \sigma_{m-1}\}$ gleichwertig ist. *Nun zeigt man, dass die in $H(\Sigma, \sigma)$ vorkommenden $\Pi O'^{\alpha_i}_i \Pi \left(\sigma_{i,0}\, \sigma_{i,1} \ldots \sigma_{i,\frac{m}{m}-1}\right)$ eine analoge, bei Transformation mit C ungeänderte Untergruppe* von

$$\left\{\bar{O}'^{k}_0 \left(\sigma_{0,0}\, \sigma_{0,1} \ldots \sigma_{0,\frac{m}{m}-1}\right), \bar{O}'^{k}_1 \left(\sigma_{1,0}\, \sigma_{1,1} \ldots \sigma_{1,\frac{m}{m}-1}\right), \ldots\right\}$$

$$(k = 1, 2, \ldots, p-1)$$

ist. Es sei

$$O = O'^{k}_0 \cdot \left(\sigma_{0,0}\, \sigma_{0,1} \ldots \sigma_{0,\frac{m}{m}-1}\right)^{\frac{p-1}{d}} \ldots$$

eine Operation mit der kleinsten, möglichen Potenz $\frac{p-1}{d}$ von $\sigma_{0,0}\, \sigma_{0,1} \ldots \sigma_{0,\frac{m}{m}-1}$. Dann kann man immer in jeder Operation O' der $H(\Sigma, \sigma)$

$$\bar{O}'^{\alpha_i}_i \left(\sigma_{i,0}\, \sigma_{i,1} \ldots \sigma_{i,\frac{m}{m}-1}\right)^{\beta_i} = \bar{O}'^{x}_i \cdot \left\{\bar{O}'^{k}_i \left(\sigma_{i,0}\, \sigma_{i,1} \ldots \sigma_{i,\frac{m}{m}-1}\right)^{\frac{p-1}{d}}\right\}^{\beta_i \cdot \frac{p-1}{d}}$$

setzen. Da nun eine Operation in $H(\Sigma, \sigma)$ vorkommt, und zwar $\{C^{-i} O C^i\}^{\beta_i \cdot \frac{p-1}{d}}$, welche in $\Sigma_{i,j}$ und $\sigma_{i,j}$[1] bis auf O'^{x}_i mit O' übereinstimmt, so muss $x = 0$ sein und unsere Behauptung ist erwiesen. *Es ist also schliesslich*

$$H(\Sigma, \sigma) = \left\{H(\Sigma), H\left(\bar{O}'^{k}_i \left(\sigma_{i,0}\, \sigma_{i,1} \ldots \sigma_{i,\frac{m}{m}-1}\right)^{\frac{p-1}{d}}\right)\right\},^{2}$$

---

[1] von Operationen in $H(\Sigma)$ abgesehen.

[2] $O'i$ kann durch Transformation wie im ersten Falle entfernt werden.

wo $H\left(\bar{O}_i^{\prime k}\left(\sigma_{i,0}\dots\sigma_{i,m-1}\right)^{\frac{p-1}{d}}\right)$ aus der in $\{\sigma_0,\sigma_1,\dots,\sigma_{m-1}\}$ enthaltenen $H(\sigma)$ durch den hervorgehobenen Ersatz des Arguments erhalten wird. Zusammenfassend können wir sagen: *Die Bestimmung von $H(\Sigma,\sigma)$ ist immer auf das frühere Problem, die Bestimmung von $H(\Sigma)$, zurückführbar.*

Nachtrag zu (15), (15′).

Die Bedingungen S. 12 gelten für alle n. Man findet für die Primzahlpotenzordnung n^i (n und m teilerfremd) als einzige, in $\overset{(i)}{H}_{n^i\varphi(m)}$ (zugehöriger Faktor: $X_{\varphi(m)}$) enthaltene und bei allen Indicesvertauschungen $i'\equiv g\,i\,(\mathrm{mod.}\ m)$ invariante Op.

$$\bar{O}=\Pi\Sigma_i^{k a_i}=\Pi\Sigma_{i_1,i_2,\dots,i_r}^{k a_i},\quad k=1,2,\dots,n^i-1;$$

$$i\equiv i_1\cdot\frac{m}{p_1}+i_2\cdot\frac{m}{p_2}+\dots+i_r\cdot\frac{m}{p_r}(\mathrm{mod.}\ m),\ i_1=0,1,\dots,p_1-1\ \text{u.s.w.}$$

$\alpha_i=1$, wenn $i_1,i_2,\dots$ alle $\neq 0$; sind aber μ etwa $i_k,i_l,\dots=0$, ist $\alpha_i=(-1)^\mu(p_k-1)(p_l-1)\dots$ zu setzen. Da $\bar{O}$ in der Form $O_1^*O_2^*\dots\overset{\varphi(m)}{\overset{\frown}{O^*_{\varkappa}}}$[1] darstellbar ist (S. 43, III), folgt leicht, dass jede $\overset{(i)}{H}_{n^{i\varkappa}}$ nur n^i-1 O^* enthält. Davon haben wir aber den Beweis von (15), (15′) abhängig gemacht. Wie man, wenn diese O^* gefunden sind, zu einer O^* für jeden Teiler m_1 von m herabsteigt, ist S. 16 ff. gezeigt.

[1] Eine O^* aus jeder $\overset{(i)}{H}_{n^{i\varkappa}}$ in $\overset{(i)}{H}_{n^i\varphi(m)}$ (S. 11 Fussnote 2 und S. 42, II).

Tryckt den 17 mars 1913.

Uppsala 1913. Almqvist & Wiksells Boktryckeri-A.-B.